TP-LINK®

二层网管交换机

TL-SG3109/TL-SL3452

用户手册

Rev2.0.2
1910040113

声明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目 录

物品清单

小心打开包装盒，检查包装盒里应有的配件：

- 一台交换机
- 一根交流电源线
- 带有 DB-9 连接器的串口线
- 一套《用户手册》及光盘
- 一张保修卡
- 两个用来将交换机固定在机架上的 L 型支架及其它配件

如果发现包装箱内有任何物品的缺失或损坏，请立即与销售该产品的经销商或者与最近的本公司的销售人员联系。

WEB 界面用户手册

前言

内置 WEB 系统是一种网络管理系统。TP-LINK 内置 WEB 界面可以通过远端浏览器对网络设备进行配置、监控和故障检测。此界面的 WEB 页面易于使用和操作。另外，此界面提供实时更新的图形和 RMON 统计信息以帮助系统管理员监控网络，在本用户手册中将以TL-SG3109为例进行说明。前言部分概述了本手册的主要内容，包含以下主题：

- 概述
- 面向的读者

概述

本手册分为以下章节，对配置和管理本系列 TP-LINK 交换机提供了详细的信息。

第一章：开始。提供使用内置 WEB 系统的信息，包括内置 WEB 界面、管理和添加、修改、删除设备的信息按钮。

第二章：配置设备信息。提供打开设备、定义一般系统特征和使用超长帧的信息。

第三章：配置系统时间。提供配置系统时间参数的信息，包括夏令时和简单网络时间协议（SNTP）。

第四章：配置系统日志。提供使用和定义系统日志的信息。

第五章：设备安全配置。提供配置设备安全方面的信息，包括安全管理、流量控制和网络安全。

第六章：定义 IP 地址。提供定义设备 IP 地址、地址解析协议和域名服务的信息。

第七章：接口配置。提供配置系统接口、端口、链路聚合组（LAG）和链路聚合控制协议（LACP）的信息；提供配置和管理 VLAN 的信息，包括 VLANGARP 和 VLANGVRP。

第八章：定义传输数据库。提供配置和管理静态和动态 MAC 地址的信息。

第九章：配置生成树协议。提供配置生成树的协议，包括快速生成树协议（RSTP）和多重生成树协议（MSTP）。第十章：配置组播转发。提供组播转发的信息。第十一章：配置 SNMP 管理。提供简单网络管理协议的管理的信息，包括定义

SNMPV1、V2c、V3 版本、SNMP 的过滤和通告。第十二章：配置服务质量。提供在设备上配置服务质量的参数。第十三章：管理系统文件。提供下载、上传和复制系统文件的信息。第十四章：设备诊断。提供端口监控、铜缆和光缆的检测、设备运行状况方面的信息。

第十五章：查看统计信息。提供设备统计的信息，包括网络远端监控统计和历史事件查询。

面向的读者

本手册面向熟悉 IT 概念和网络术语的网络管理员。

第1章　开始

这一部分介绍用户界面的知识，包含以下主题：

- 使用 TP-LINK 内置 WEB 界面前所需的配置
- 启用 TP-LINK 内置 WEB 界面
- 理解 TP-LINK 内置 WEB 界面
- 页面和表单的使用
- 设备复位
- 从设备上注销登录

1.1 使用TP-LINK内置WEB界面前所需的配置

交换机出厂时 WEB 管理界面默认是不能使用的。用户必须先通过命令行接口（CLI）对交换机进行一些配置，下面介绍详细的配置步骤。

1. 使用交换机附带的串口线，将交换机上的 Console 口与 PC 机串口连接。
2. 运行 Windows 中自带的“超级终端”程序。Windows 中“超级终端”所在的路径一般是：开始菜单>程序>附件>通讯>超级终端。
3. 当出现如下图所示的“连接到”对话框时，选择与交换机连接的串口。如果是 PC 上的第 1 个串口，则选择“COM1”，依此类推。单击“确定”到下一步。

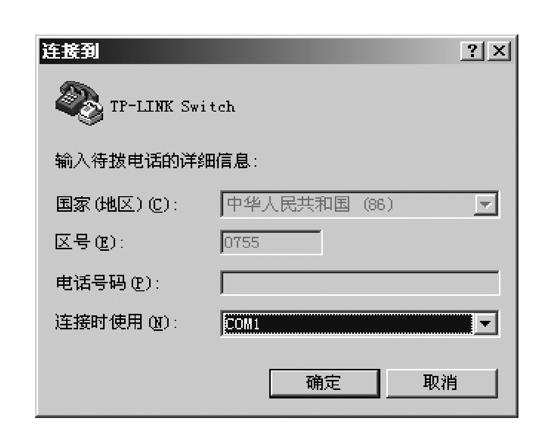


图 1-1

4. 当出现“COM1 属性”对话框时，设置每秒位数为 38400，数据位为 8，无奇偶校验，停止位为 1，无数据流控制。单击“确定”完成超级终端的设置。



图 1-2

5. 接通交换机电源，超级终端上会出现交换机启动并进行上电自检的信息。约 1 分钟后，交换机启动完成，按“Enter”键，超级终端上出现命令行接口的命令提示符“console>”，表明交换机的命令行接口已准备好接收命令输入。如下图所示：

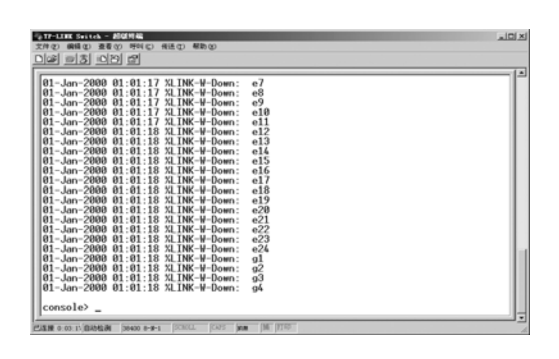


图 1-3

6. 要使用 WEB 界面管理交换机，需为默认 VLAN 设置一个 IP 地址和子网掩码，以及添加一个具有最高特权级（级别 15）的超级用户。下面是一个在超级终端上输入命令的例子：

console> **enable**

console# **configure**

console(config)# username admin password admin level 15

console(config)# **interface vlan 1**

console(config-if)# ip address 192.168.1.1 255.255.255.0

console(config-if)# **exit**

console(config)# **exit**

console# copy running-config startup-config

01-Jan-2000 01:02:49 %COPY-I-FILECPY: Files Copy-source URL running-config destination URL flash://startup-config

01-Jan-2000 01:02:50 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded

上面的示例配置了如下的内容：

- 第 3 行命令添加了一个特权级为 15 的用户，用户名和密码都是“admin”，也可以配置其他用户名和密码。这里设置的用户名和密码就是使用 WEB 界面管理时登录用的用户名和密码。
- 第 5 行命令为默认的 VLAN 配置了 IP 地址 192.168.1.1，子网掩码是 255.255.255.0。这里的 IP 地址和子网掩码设置需保证跟 PC 机的 IP 地址在同一个子网中。
- 第 8 行命令将上述配置保存到交换机的启动配置中，这样交换机断电后上述配置仍保存在交换机内部。

经过上述配置之后，就可以使用WEB界面对交换机进行管理了。打开WEB浏览器，在地址栏中输入 “http://192.168.1.1/”，就可以打开交换机的内置WEB界面，并可以使用“admin”作为用户名和密码登录。

本手册的《交换机初始配置指南》部分对交换机的初始配置进行了更为详尽的描述，可在使用 WEB 界面之前参考之。

1.2 启用TP-LINK内置WEB界面

这部分包括启用 TP-LINK 内置 WEB 界面的信息。

☞ 注意：
在使用TP-LINK内置WEB界面配置设备之前，请关闭浏览器阻止弹出窗口的功能。如果使用Microsoft Internet Explorer浏览器，需用该浏览器的 6.0 或更高版本。

访问 TP-LINK 用户界面的步骤：

1、打开 WEB 浏览器。

2、确保浏览器阻止弹出窗口的功能已关闭。如果未关闭，修改、添加和设备信息项窗口可能打不开。

3、在浏览器地址栏中输入 IP 地址，按回车键打开登录页面：



图 1-4 登录页面

4、 输入用户名和密码。

☞ 注意：

- 输入密码时需注意字母的大小写。
- 关闭浏览器阻止弹出窗口的功能。
- 默认的密码可通过命令行接口(CLI)进行设置，请参考《CLI参考指南》。

5、 点击“确定”。打开 TP-LINK 内置 WEB 界面首页：

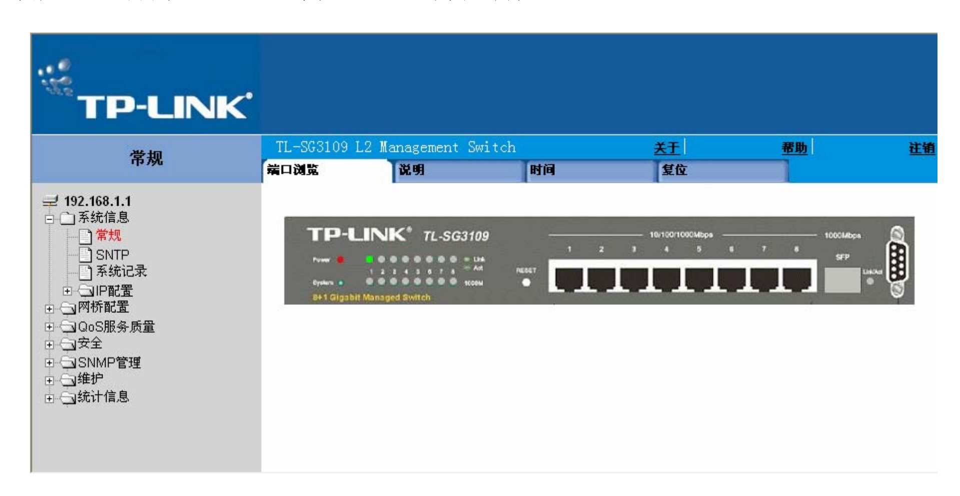


图 1-5 TP-LINK 内置 WEB 界面首页

TP-LINK 内置 WEB 界面首页包含以下主题：

- 端口 LED 指示灯：位于页面的顶端。这里用图形表示 TP-LINK 交换机前面板上端口 LED 指示灯的状态。
- Tab 区：位于 LED 指示灯上面。Tab 区包括一系列的设备功能组件。
- 设备视图：位于页面的主体部分。提供设备的图形表示、信息和表单或者配置功能。

1.3 理解TP-LINK内置WEB界面

下表列出了用户界面的组件：

组件	描述
树形图	通过树形图可以方便地浏览设备的可配置特性。主节点可以展开并显示多个子节点。
设备视图	设备视图提供设备端口，当前配置和状态，表单信息，特性组件等方面的信息。设备还显示其他设备信息，并提供对话框对设备参数进行配置。
Tab 区	Tab 区提供在不同的设备特性间切换的功能。单击一个 Tab 可以查看或配置该特性里面的所有组件。
全局图	提供 TP-LINK 交换机的一个图形化表示。
关于和帮助	提供内置 Web 系统的信息和联机帮助。

表 1-1 界面组件

这部分提供了以下附加信息：

- 设备表示：提供用户界面按钮的解释，包括管理按钮和任务图标。
- 使用内置 WEB 界面管理按钮：提供添加、修改和删除配置参数的指导。

1.3.1 设备表示

内置 WEB 界面首页包含设备图形化的表示。这种表示根据设备平台而不同。



图 1-6 设备的表示

☞ **注意：**

本手册中的所示的界面截图都是以TL-SG3109交换机为例的。对本系列的其他交换机，实际的界面类似。

1.3.2 使用内置WEB界面管理按钮

配置管理按钮和图表提供一种简单的配置设备信息的方法，包含以下：

按钮	按钮名称	描述
上一页 下一页	上一页/下一页	用于浏览表单的条目
清空日志	清空日志	清除系统日志
创建	创建	用于创建配置项
	修改	修改配置
查询	查询	查询表单
复位	复位	复位设备
保存	保存	保存当前的系统配置
提交	提交	将配置改动保存到设备中
开始测试	开始测试	进行线缆测试

表 1-2 TP-LINK WEB 界面管理按钮

Tab	Tab 名称	描述
帮助	帮助	打开联机帮助
注销	注销	打开注销登录页面

表 1-3 WEB 界面信息按钮

1.4　页面和表单的使用

TP-LINK WEB 界面包含多个表单和页面用来对设备进行配置。

这部分包括以下主题：

- 添加配置信息
- 修改配置信息
- 删除配置信息

1.4.1　添加配置信息

用户定义的信息可以通过打开一个新的添加界面添加到特定的内置 WEB 界面页面。

添加信息到表单或者 WEB 页面：

1、 点击：系统信息>IP 配置>IP 定址>IP 接口。

2、 点击“创建”，打开添加 IP 接口页面：



图 1-7 添加 IP 接口页面

3、 填入必要的信息。

4、 点击“提交”。存储配置信息，更新设备。

1.4.2　修改配置信息

用户定义的信息能够通过打开一个新的设置页面在特定的内置 WEB 界面页面进行修改。

在表单或者内置 WEB 界面页面上修改信息：

1、 点击：系统信息>IP 配置>IP 定址>IP 接口。

2、 点击 ，打开 IP 接口设置页面：

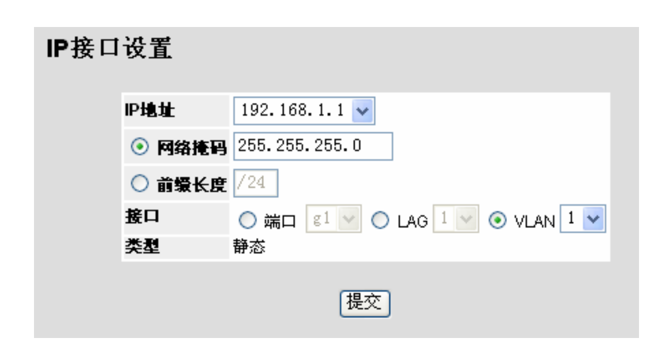


图 1-8 IP 接口设置页面

3、 修改。

4、 点击“提交”。存储设置，更新设备。

1.4.3 删除配置信息

用户定义的信息可以在特定的 WEB 界面页面上使用删除功能进行删除。

删除表单或者内置 WEB 界面页面上的信息：

1、 点击：系统信息>IP 配置>IP 定址>IP 接口，打开 IP 接口页面：



图 1-9 IP 接口页面

2、 在要删除的项目一栏选中删除复选框。

3、 点击“提交”。信息删除，设备更新。

1.5 设备复位

在复位页面上能够进行从远端复位设备的操作。

☞ 注意：

为了防止当前的配置信息丢失，在复位设备之前，把正在运行的配置文件的改变信息存储到启动配置文件中。相关指令，请参照 13.4 节的“复制系统文件”部分。

设备复位：

1、 点击：系统信息>常规>复位，打开复位页面：



图 1-10 复位页面

2、 点击“复位”。弹出确认框。



图 1-11 重启确认

3、 点击“确定”。弹出对话框。

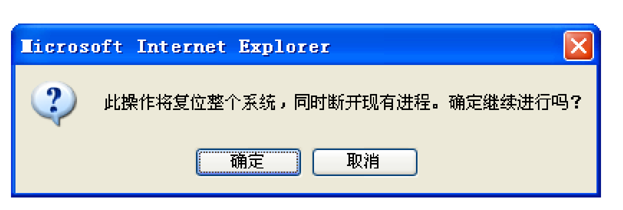


图 1-12 复位确认

4、 点击“确定”，设备复位。

5、 重新登录，输入用户名和密码，重新连接 WEB 界面。

1.6 从设备上注销登录

点击“注销”。弹出退出确认对话框。



图 1-13 退出确认信息

第2章　　配置设备信息

这部分内容包含查看和设置一般系统信息。

系统信息页面包含配置设备信息的一些参数，包括产品名称、系统名称、系统位置、系统联系人、系统对象 ID、系统运行时间、本机 MAC 地址、硬件版本、软件版本和引导程序版本。

查看和定义系统信息：

1、 点击：系统信息>常规>说明，打开系统信息页面：



图 2-1 系统信息页面

系统信息页面包含以下字段：

- 产品名称-显示设备的机型名称。
- 系统名称-用户自定义的系统名字。此项可输入 0 到 160 个字符。
- 系统位置-设备所处的地理位置。此项可输入 0 到 160 个字符。
- 系统联系人-系统管理员的联系信息。此项可输入 0 到 160 个字符。
- 系统对象 ID-显示厂家网络管理子系统的权威认证。
- 系统运行时间-显示系统最近一次重启以来连续运行的时间。系统时间采用的格式为天、小时、分钟、秒。例如，41 天 2 小时 22 分钟 15 秒。
- 本机 MAC 地址-显示设备的物理地址（MAC 地址）。
- 硬件版本-显示设备的硬件版本号。
- 软件版本-显示设备当前的软件版本号。
- 引导程序版本-显示当前的引导程序版本号。

2、 定义系统名称，系统位置及系统联系人。

3、 点击“提交”，系统的描述情况被存储，设备更新。

第3章　配置系统时间

本章提供配置系统时间参数的信息，包括：

- 配置夏令时时间
- 配置 SNTP

3.1 配置夏令时时间

系统信息时间页面包括为本地硬件系统时钟和外部 SNTP 时钟定义时间参数部分。如果系统时间始终使用外部 SNTP 时钟且外部 SNTP 时钟出错，系统时间将恢复到本地硬件时钟。可以在设备上启用夏令时。

下面是夏令时在指定国家和地区的开始和终止时间列表：

- 阿尔巴尼亚：从三月最后一个周末到十月最后一个周末。
- 澳大利亚：从十月底到三月底。
- 澳大利亚：塔斯马尼亚岛,塔斯马尼亚州-从十月开始到三月底。
- 亚美尼亚：从三月最后一个周末到十月最后一个周末。
- 匈牙利：从三月最后一个周末到十月最后一个周末。
- 巴哈马群岛：从四月到十月，与美国的夏令时一起。
- 白俄罗斯：从三月最后一个周末到十月最后一个周末。
- 比利时：从三月最后一个周末到十月最后一个周末。
- 巴西：从十月第三个星期日到第二年三月第三个星期六。在夏令时期间，
- 巴西始终比巴西东南部快一个小时。
- 智利：在复活节岛，从 3 月 9 日到 10 月 12 日。在该国其他地方，从三月第一个星期六开始或 3 月 9 日之后。
- 中国：中国不使用夏令时。
- 加拿大：从四月的第一个周日到十月的最后一个周日。夏令时通常由省或地方政府调整。一些自治区除外。
- 古巴：从三月最后一个周日到十月最后一个周日。
- 塞浦路斯：从三月最后一个周末到十月最后一个周末。
- 丹麦：从三月最后一个周末到十月最后一个周末。
- 埃及：从四月最后一个周五到九月最后一个周四。
- 爱沙尼亚：从三月最后一个周末到十月最后一个周末。

- 芬兰：从三月最后一个周末到十月最后一个周末。
- 法国：从三月最后一个周末到十月最后一个周末。
- 德国：从三月最后一个周末到十月最后一个周末。
- 希腊：从三月最后一个周末到十月最后一个周末。
- 匈牙利：从三月最后一个周末到是十月最后一个周末。
- 印度：印度不使用夏令时。
- 伊朗：从 3 月 1 日到 9 月 1 日。
- 伊拉克：从 4 月 1 日到 10 月 1 日。
- 爱尔兰：从三月最后一个周末到十月最后一个周末。
- 以色列：每年都在改变。
- 意大利：从三月最后一个周末到十月最后一个周末。
- 日本：日本不使用夏令时。
- 约旦：从三月最后一个周末到十月最后一个周末。
- 拉托维亚：从三月最后一个周末到十月最后一个周末。
- 黎巴嫩：从三月最后一个周末到十月最后一个周末。
- 立陶宛：从三月最后一个周末到十月最后一个周末。
- 卢森堡：从三月最后一个周末到十月最后一个周末。
- 马其顿：从三月最后一个周末到十月最后一个周末。
- 墨西哥：从四月第一个周日两点到十月最后一个周日两点。
- 摩尔多瓦：从三月最后一个周末到十月最后一个周末。
- 门的内哥罗（黑山）：从三月最后一个周末到十月最后一个周末。
- 荷兰：从三月最后一个周末到十月最后一个周末。
- 新西兰：从十月第一个周日到第二年三月第一个周日或 3 月 15 日。
- 挪威：从三月最后一个周末到十月最后一个周末。
- 巴拉圭：从 4 月 6 日到 9 月 7 日。
- 波兰：从三月最后一个周末到十月最后一个周末。
- 葡萄牙：从三月最后一个周末到十月最后一个周末。
- 罗马尼亚：从三月最后一个周末到十月最后一个周末。。
- 俄罗斯：从三月最后一个周末到十月最后一个周末。
- 塞尔维亚：从三月最后一个周末到十月最后一个周末。

- 斯洛伐克：从三月最后一个周末到十月最后一个周末。
- 南非：南非不使用夏令时。
- 西班牙：从三月最后一个周末到十月最后一个周末。
- 瑞典：从三月最后一个周末到十月最后一个周末。
- 瑞士：从三月最后一个周末到十月最后一个周末。
- 叙利亚：从 3 月 31 日到 10 月 30 日。
- 台湾：台湾不使用夏令时。
- 土耳其：从三月最后一个周末到十月最后一个周末。
- 英国：从三月最后一个周末到十月最后一个周末。
- 美国：从四月第一个周日的两点到十月最后一个周日两点。

配置夏令时时间：

1、点击：系统信息>常规>时间，打开 SNTP 时钟时区页面：



图 3-1SNTP 时钟时区页面

SNTP 时钟时区页面包含以下字段：

- 时钟源：用来设置系统时钟的时钟源。可能的值是：
  - 本地设置：表示没有使用时钟源。时钟为本地时钟。
  - SNTP：表示通过 SNTP 服务器设置系统时间。

本地设置部分包括以下字段：

- 日期：系统日期。字段格式是日/月/年。例如：04/05/50（5 月 4 日，2050 年）。

- 本地时间：系统时间。字段格式是时：分：秒。例如：21：15：03。
- 时区偏移：本地时间和格林威治时间的差数。例如，北京的时区偏移是 GMT+8，而纽约的时区偏移是 GMT-5。
- 夏令时：在设备上启用基于设备所在地区的自动夏令时。可以根据特殊的

年份或者以每一年的重复时期来设置夏令时。对特殊年份，完成夏令时段；对重复设置，完成重复字段。

  - 美国：设备在四月第一个周六凌晨两点转换到夏令时，在十月最后一个周六凌晨两点恢复到标准时间。
  - 欧洲：设备在三月最后一个周日凌晨 1 点转换到夏令时并且在十月最后一个周末凌晨 1 点恢复到标准时间。选项欧洲应用于欧盟成员国，其他欧洲国家使用欧盟标准。
  - 其他：夏令时区定义基于设备所在的地区。如果选择了其他则必须定义从和到字段。
- 时间设置偏移：用于非美国和欧洲国家设置夏令时时间数（以分钟）。默认时间是 60 分钟。
- 从：表示除了美国和欧洲的夏令时时间的开始，一个字段的格式是日/月/年而另一个字段格式是小时：分。例如，如果夏令时开始于 2007 年 10 月 25 日凌晨 5 点，则该两个字段应该设置成 25/10/07 和 05：00。字段可能的值如下：
  - 日：夏令时开始的日期。可能的值是 1-31。
  - 月：夏令时在该年开始的月份。可能的值是 1-12 月。
  - 年：配置开始夏令时的年份。
  - 时间：夏令时开始的时间。字段格式是小时：分。例如：05：30。
- 到：表示除了美国和欧洲的夏令时结束时间，一个字段格式是日/月/年而另一个字段格式是小时：分。例如，如果夏令时在 2008 年 3 月 23 日晚上 12 点结束，该两个字段应该是 23/03/08 和 00：00。可能的字段如下：
  - 日：夏令时结束的日期。可能的值是 1-31。
  - 月：夏令时在该年结束的月份。可能的值是 1-12 月。
  - 年：配置结束夏令时的年份。
  - 时间：夏令时结束的时间。字段格式是小时：分。例如：05：30。
- 常年设置：启用除美国和欧洲外每年夏令时时间不变的国家的用户自定义的夏令时。
- 从：每年夏令时开始的时间。例如，本地区夏令时开始于每年四月第一个周六凌晨 00 点。可能的值如下：
  - 日：每年夏令时开始于周几。可能的值是周六到周六。

– 周：每年夏令时开始于一个月的第几周。可能的值是 1-5。

– 月：每年夏令时开始的月份。可能的值是 1-12 月。

– 时间：每年夏令时开始的时间。格式为小时：分。例如：02：10。

➢ 到：每年夏令时结束时间。例如，本地夏令时结束于每年十月第一个周六的午夜 12 点。可能的字段是：

– 日：每年夏令时结束于周几。可能的值是周六到周六。

– 周：周-每年夏令时结束于一个月的第几周。可能的值是 1-5。

– 月：每年夏令时结束的月份。可能的值是 1-12 月。

– 时间：每年夏令时结束的时间。格式为小时：分。例如：05：30。

2、定义日期，本地时间和时区偏移字段。

3、要配置设备自动转换到夏令时，选择夏令时并选择美国，欧洲或其他。如果选择其他，必须定义从和到字段。要配置每年重复的夏令时参数，选择常年设置和定义其从和到字段。

4、点击“提交”，保存设置，设备将会更新设置。

3.2 配置SNTP

本节包括以下主题：

➢ SNTP 概述

➢ 定义 SNTP 全局设置

➢ 配置 SNTP 认证

➢ 定义 SNTP 服务器

➢ 定义 SNTP 接口设置

3.2.1 SNTP概述

设备支持简单网络时间协议（SNTP）。SNTP 确保网络设备的时钟时间同步到毫秒。时间同步是由网络 SNTP 服务器执行。设备只运行为 SNTP 的一个客户，并且不能给其他系统提供时间服务。设备可以从以下服务器类型检测服务器时间：

➢ 单播

➢ 任意播

➢ 广播

时间源由层建立。层定义时钟的精度。层越高（零是最高），精度越高。设备从第一层或更高层接收时间。

以下是层的一个例子：

- 层 0：以实时钟（比如 GPS 系统）作为时间源。
- 层 1：直接连接到层 0 的服务器作为时间源。层 1 的时间服务器提供主要的网络时间标准。
- 层 2：时间源经过网络远离层 1 服务器。例如，层 2 服务器在网络上通过 NTP，从层 1 服务器接收时间。

从 SNTP 服务器接收的信息通过时间级别和服务器类型来评估。由以下的时间级别来评估和决定 SNTP 时间精度：

- T1：客户发出原始请求的时间
- T2：服务器接收到原始请求的时间
- T3：服务器发送应答给客户的时间
- T4：客户收到服务器应答的时间

3.2.1.1 检测单播时间信息

检测单播信息用在检测一个已知 IP 地址的服务器。T1-T4 被用来测定服务器时间。这是同步设备时间的首选方式。

3.2.1.2 检测任意播时间信息

检测任意播信息用在 SNTP 服务器 IP 地址未知的情况下。第一个任意播服务器返回的响应用来设置时间值。时间级别 T3 和 T4 用来确定服务器时间。使用任意播时间信息同步设备时间优先于使用广播时间信息。

3.2.1.3 检测广播时间信息

广播信息用在服务器 IP 地址未知的情况下。当 SNTP 服务器发出广播信息后，SNTP 客户端侦听响应。SNTP 客户端既不发送时间信息请求也不从广播服务器接收响应。

消息摘要 5（MD5）认证维护到 SNTP 服务器的同步路径。MD5 是一种产生 128 位散列值的算法。它是 MD4 的一个变种并且提高了 MD4 的安全性。MD5 检验通讯的完整性和鉴别信源。

3.2.2 定义SNTP全局设置

SNTP 属性页面提供定义 SNTP 全局参数的信息。

定义 SNTP 全局参数：

1、 点击：系统信息>SNTP>属性，打开 SNTP 配置页面：



图 3-2 SNTP 配置页面

SNTP 配置页面包括以下字段：

➢ 轮询间隔：定义 SNTP 服务器被单播信息检测的时间间隔（秒）。轮询间隔默认是 1024 秒。

➢ 启用接收广播服务器更新：定义设备在选定的接口上总是以广播服务器时间信息监控 SNTP 服务器。可能的值为：

 – 启用：启用设备接收广播服务器更新。

 – 禁用：禁止设备接收广播服务器更新。

➢ 启用接收任意广播服务器更新：定义总是以任意播服务器时间信息检测 SNTP 服务器。

➢ 启用接收单播服务器更新：定义设备总是以单播服务器时间信息检测 SNTP 服务器。如果接收广播服务器更新，接收任意播服务器更新和接收单播服务器更新字段都是启用的，系统时间根据单播服务器时间信息设置。可能的值为：

 – 启用：启用设备接收单播服务器更新。

 – 禁用：禁止设备接收单播服务器更新。

➢ 启用轮询单播服务器：定义设备总是发送 SNTP 单播转发信息给 SNTP 服务器。可能的值是：

 – 启用：起用设备接收检测单播服务器更新。

 – 禁用：禁止设备接收检测单播服务器更新。

2、定义轮询间隔，对上述四个“启用”字段：启用接收广播服务器更新，启用接收任意广播服务器更新，启用接收单播服务器更新和启用轮询单播服务器，选择至少一个启用字段。

3、点击“提交”，则 SNTP 全局设置就被定义了，并且设备被更新。

3.2.3 配置SNTP认证

SNTP 认证页面启用配置 SNTP 认证方法。

配置 SNTP 认证：

1、 点击：系统信息>SNTP>认证，打开 SNTP 认证页面：



图 3-3 SNTP 认证页面

SNTP 认证页面包括以下字段：

➢ 启用 SNTP 认证：表示是否认证在设备和 SNTP 服务器间的 SNTP 会话是启用的。可能的值有：

– 选中：启用认证在设备和 SNTP 服务器之间 SNTP 会话。

– 不选中：禁止认证在设备和 SNTP 服务器间的 SNTP 会话。

➢ 密钥 ID：表示是否用加密密钥来认证 SNTP 服务器和设备。该字段最大值为 4294967295。

➢ 认证密钥：表示认证用的密钥。

➢ 信任密钥：表示使用（单播/任意播）/选中（广播）来认证 SNTP 服务器的加密密钥。

➢ 删除：移除加密密钥 ID。可能的值是：

– –选中：移除选择的加密密钥 ID。

– –不选中：维持加密密钥 ID。这是默认值。

2、 选中启用 SNTP 认证复选框。

3、 点击“提交”，定义 SNTP 认证，设备将更新。

定义 SNTP 认证参数：

1、 点击“创建”，打开添加 SNTP 认证页面：

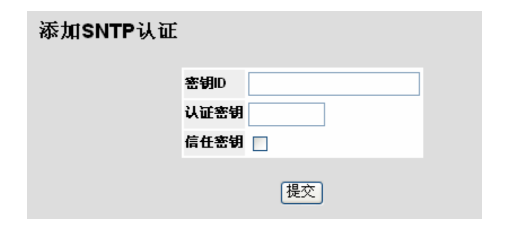


图 3-4 添加 SNTP 认证页面

2、 定义密钥 ID，认证密钥和信任密钥字段。

3、点击“提交”，添加认证密钥和更新设备。

3.2.4 定义SNTP服务器

SNTP 服务器页面包括启用 SNTP 服务器，添加新的 SNTP 服务器信息。另外，SNTP 服务器页面也可启用设备请求和接收 SNTP 服务器通信。

定义 SNTP 服务器：

1、点击：系统信息>SNTP>服务器，打开 SNTP 服务器页面：



图 3-5 SNTP 服务器页面

SNTP 服务器页面包括以下字段：

- SNTP 服务器：显示用户定义的 SNTP 服务器 IP 地址。最多可以定义 8 个 SNTP 服务器。
- 轮询间隔：显示设备为系统时间信息检测 SNTP 服务器的间隔。
- 密钥 ID：显示用于在设备和 SNTP 服务器间通信的加密密钥识别符。该字段范围是 1-4294967295。
  - 首选项：表示提供 SNTP 系统时间的优先 SNTP 服务器。可能的值为：
  - 主要：表示提供 SNTP 信息的主服务器。
  - 次要：表示提供 SNTP 信息的候选服务器。
- 状态：SNTP 服务器的运行状态。可能的值为：
  - –正常：表示 SNTP 服务器正在正常运行。
  - –关闭：表示 SNTP 服务器当前不可用。例如，SNTP 服务器未连接或者已关闭。
  - –运行：表示 SNTP 服务器正在发送或接收 SNTP 信息。
  - –未知：表示当前正在发送的 SNTP 信息未知。例如，设备正在查找接口。

- 上一次响应：显示从 SNTP 服务器收到的最后一个响应的时间。
- 偏移：表示设备本地时钟与已从 SNTP 服务器获得的时钟的时间差。
- 延迟：表示设备请求到达 SNTP 服务器的时间总数
- 删除：从 SNTP 服务器列表移除 SNTP 服务器。可能的值为：
  - 选中：移除 SNTP 服务器。
  - 不选中：维持 SNTP 服务器。这是默认值。

2、 点击“创建”，打开添加 SNTP 服务器页面：



图 3-6 添加 SNTP 服务器页面

3、 定义 SNTP 服务器，启用轮询间隔和密钥 ID 字段。

4、 点击“提交”，添加 SNTP 服务器，设备更新。

3.2.5 定义SNTP接口设置

SNTP 接口设置页面包括在不同的接口上设置 SNTP 的字段。

定义 SNTP 接口设置：

1、 点击：系统信息>SNTP>接口，打开 SNTP 接口页面：



图 3-7 SNTP 接口页面

SNTP 接口页面包括以下字段：

➢ 接口：表示在哪个接口上可以启用 SNTP。可能的值为：

– 端口：表示在指定的端口号上启用 SNTP。

– LAG：表示在指定的 LAG 号上启用 SNTP。

– VLAN：表示在指定的 VLAN 号上启用 SNTP。

接收服务器更新：启用服务器接收或不接收更新。

删除：移除 SNTP 接口。

– 选中：移除选择的 SNTP 接口

– 不选中：维持定义的 SNTP 接口。

2、点击“创建”，打开添加 SNTP 接口页面。



图 3-8 添加 SNTP 接口页面

3、选择接口。

4、选中接收服务器更新复选框。

5、点击“提交”，添加 SNTP 接口，更新设备。

第4章　配置系统日志

本章提供管理系统日志的信息。系统日志使得实时查看设备的事件成为可能，并能记录这些事件供稍后查看。系统日志负责记录和管理事件，并报告错误和提示信息。

事件消息有唯一的格式，所有的错误报告都按照 Syslog 协议推荐的消息格式。例如，每条系统日志和本地设备报告消息都被分配一个严重性级别代码，并且包括一个用于识别产生消息的源应用程序的消息记忆符号，这样就可以通过消息的紧急和关联程度来对它们进行过滤。每个消息严格测定发送每个消息的设备的事件日志集合。

下表列出日志的严重性级别：

严重性	级别	消息
紧急	0(最高)	系统不能工作
警惕	1	系统需要立即注意
危险	2	系统处于危险状态
错误	3	产生一个系统错误
警告	4	产生一个系统警告
注意	5	系统正常运行，但产生了一个注意通告
通知	6	提供设备信息
调试	7	提供日志的细节信息。如果产生了一个调试错误，联系客户技术支持。

表 4-1 系统日志严重性级别

本章包含以下主题：

- 定义一般日志属性
- 查看内存日志
- 查看闪存日志
- 定义系统日志服务器

4.1　定义一般日志属性

系统日志属性页面包含定义哪些事件记录到哪些日志的字段。包括启用全局日志字段和定义日志的参数。日志消息按照严重性级别从最高到最低列出。

查看系统日志属性：

1、 点击：系统信息>系统记录>属性，打开日志设置页面：



图 4-1 日志设置页面

日志设置页面包括以下字段：

➢ 启用日志：表示启用设备的全面记录内存、闪存和服务器日志。终端日志默认是启用的。可能的值是：

  – 选中：启用设备日志。

  – 不选中：禁用设备日志。

➢ 事件类别：以降序列出事件类型级别。启用选择最低事件类型。

☞ 注意：

当选择了一种严重性级别，更高的所有严重性级别都将自动选择。

  ➢ 终端：定义发送给控制台的日志的最低严重性级别。

  ➢ 内存日志：定义发送到RAM并保存在RAM（缓存）中的日志的最低严重性级别。

  ➢ 闪存日志：定义发送到日志文件并保存在闪存中的日志的最低严重性级别。

2、 选中启用日志复选框。

3、 选中终端、内存日志、闪存日志的严重性级别复选框。

4.2 查看内存日志

内存页面包含所有保存在 RAM（缓存）中的按时间发生顺序排列的系统日志。

查看内存日志：

1、 点击：系统信息>系统记录>内存，打开内存页面：



图 4-2 内存页面

内存页面包含以下字段：

- 日志目录：列出日志编号。
- 日志时间：列出日志加入的日期和时间。
- 事件类别：列出日志加入时事件的严重性。
- 说明：列出事件描述。

2、 清除所有日志，点击“清空日志”。

3、 点击“确定”，从表中移除所有日志条目，更新设备。

4.3 查看闪存日志

闪存页面包含保存到闪存的日志文件的条目信息，包括产生日志的时间，日志的严重性和日志消息的描述。在重新启动设备后消息日志处于可用状态。

查看闪存日志：

1. 点击：系统信息>系统记录>闪存，打开闪存页面：



图 4-3 闪存页面

闪存页面包含以下字段：

- 日志目录：列出日志索引号。
- 日志时间：列出日志加入的日期和时间。
- 事件类别：列出在闪存中创建的日志事件的严重性。
- 说明：列出事件描述。
  - 清除当前闪存日志，点击“清空日志”。
  - 点击“确定”，从表中清除日志。

4.4 定义系统日志服务器

远程日志页面包含查看和配置远端日志服务器的信息。可以定义新的日志服务器和发送给每个服务器的日志严重性。

定义系统日志服务器：

1、 点击：系统信息>系统记录>服务器，打开远程日志页面：



图 4-4 远程日志页面

远程日志页面列出服务器参数和包含以下字段：

- 服务器：指定可以发送日志的服务器。
- UDP 端口号：定义向服务器发送日志的 UDP 端口。可能的端口范围是 1-65535.默认值为 514。
- 设备：定义发送系统日志给远端服务器的应用程序。一个服务器只能分配一个设备。如果定义了第二个设备级别，第一个设备将被取代。设备定义的所有应用在服务器上利用同一个设备。字段默认是本地 7。可能的字段值是本地 0-本地 7。
- 说明：提供用户定义的服务器的描述。
- 最小事件类别：表示发送给服务器的日志的最低严重性。例如，如果选择了注意，所有具有注意和高于这个级别的日志都将被发送到远端服务器。

➢ 删除：从服务器列表删除当前选择的服务器。可能的值是：

– 选中：从系统属性页面中移除选择的服务器。一旦移除，日志将不再被发送到远端服务器。

– 不选中：维持远端服务器。

2、 点击“创建”，打开添加系统日志服务器页面：

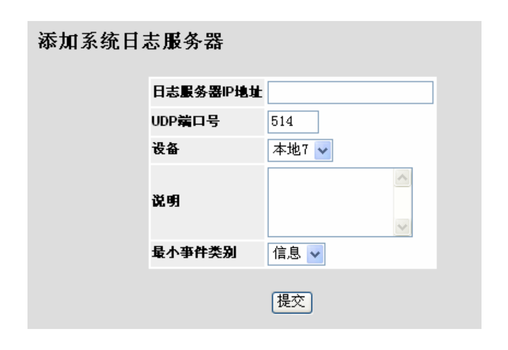


图 4-5 添加系统日志服务器页面

3、 定义日志服务器 IP 地址，UDP 端口号，设备，说明和最小事件类别。

4、 点击“提交”，定义日志服务器和更新设备。

第5章　　设备安全配置

本章描述了如何设置 TP-LINK 设备的端口安全参数、设备管理方法、用户配置和服务器安全。本章包含以下主题：

- 管理安全配置
- 网络安全配置

5.1 管理安全配置

提供管理安全配置的相关信息。该部分包含以下主题：

- 认证方法配置
- 密码配置

5.1.1 认证方法配置

提供设备认证方法配置的相关信息。该部分包含以下主题：

- 定义访问配置文件
- 定义配置文件规则
- 定义认证配置文件
- 映射认证配置文件
- TACACS+主机设置
- RADIUS 服务器设置

5.1.1.1 定义访问配置文件

访问配置文件是用以访问设备的配置文件和规则。对于管理功能的访问可以被限制于用户组。用户组依据接口的 IP 地址和 IP 子网进行定义。访问配置文件中包含了用来对访问和管理的管理方式。这些方式包括：

- 全部
- Telnet
- Secure Telnet(SSH)
- HTTP
- Secure HTTP(HTTPS)
- SNMP

管理方式可根据用户组的不同而不同。例如，用户组 1 只能通过 HTTPS 会话对交换模块进行管理，而用户组 2 则可以同时通过 HTTPS 或 Telnet 会话对交换模块进行管理。访问配置文件页面包含了当前已访问配置文件及其状态。

若将访问配置文件分配至某个特定的端口，则其他端口的访问将被拒绝。如果一个访问配置文件被分配至“任意端口”，则所有端口均能对设备进行访问。

配置访问配置文件：

1、 点击：安全>管理安全>认证>访问配置文件，打开访问配置文件页面：



图 5-1 访问配置文件页面

访问配置文件页面包含以下字段：

访问配置文件名：定义访问配置文件的名称。该名称可包含最多 32 个字符。

当前活动的访问配置文件：定义当前启用的配置文件

删除：删除所选择的访问配置文件。可选择：

– 选中：删除已选的访问配置文件（不能删除当前处于启用的状态的访问配置文件）

– 不选中：保留该访问配置文件

2、 单击“创建”，打开添加访问配置文件页面：



图 5-2 添加访问配置文件页面

添加访问配置文件页面包含以下字段：

- 访问配置文件名：定义访问配置文件的名称

- 规则优先级：定义规则的优先级。当数据包匹配某条规则时，则用户组对设备的访问将被允许或拒绝。由于数据包与规则的匹配遵循“First-fit”原则，故规则的编号至为重要。对于规则的优先级需在配置文件规则页面中进行指定。

- 管理方式：定义已定义规则的管理方式。使用该访问配置文件的用户可通过所指定的管理方式对设备进行访问。可选择的管理方式有：

  – 全部：指定该规则可以使用所有的管理方式。

  – Telnet：指定该规则使用 Telnet 管理方式。若选择该方式，使用 Telnet 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝。

  – SecureTelnet（SSH）：指定该规则使用 SSH 管理方式。若选择该方式，使用 Telnet 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝

  – HTTP：指定该规则使用 HTTP 管理方式。使用 HTTP 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝。

  – Secure HTTPS：指定该规则使用 HTTPS 管理方式。使用 HTTPS 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝。

  – SNMP：指定该规则使用 SNMP 管理方式。使用 SNMP 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝。

- 接口：定义已定义访问配置文件使用的接口。可选择：

  – 端口：指定已定义访问配置文件使用的端口。

  – LAG：指定已定义访问配置文件使用的 LAG。

  – VLAN：指定已定义访问配置文件使用的 VLAN。

- 源 IP 地址：指定已定义访问配置文件使用的接口源 IP 地址，且源 IP 地址可

以是子网的 IP 地址。

  – 网络掩码：指定源 IP 地址的网络掩码。

  – 前缀长度：指定源 IP 地址前缀或网络掩码的位数。

操作：定义访问规则所采用的动作。可选择：

  – 允许：允许对设备的访问。

  – 拒绝：拒绝对设备的访问。此为缺省值。

3、 点击“提交”，保存访问配置文件并更新系统。

5.1.1.2 定义配置文件规则

访问配置文件最多能设置 128 条规则用以决定哪些用户可通过那些方式来管理交换模块。同时用户对设备的访问也可能被拒绝。这些规则由各种过滤器组成，它们包括：

- 优先级
- 接口
- 管理方式
- 源 IP 地址
- 前缀长度
- 操作

定义配置文件规则：

2. 点击：安全>管理安全>认证>配置文件规则，打开配置文件规则页面：



图 5-3 配置文件规则页面

配置文件规则页面包含以下字段：

- 访问配置文件名：显示当前规则所绑定的访问配置文件
- 优先级：定义规则的优先级。当数据包匹配某条规则时，则用户组对设备的访问将被允许或拒绝。由于数据包与规则的匹配遵循“First-fit”原则，故规则的编号至为重要。
- 接口：表示应用该规则的接口的类型。可选项有：
  - 端口：将该规则绑定于选定的端口
  - LAG：将该规则绑定于选定的 LAG
  - VLAN：将该规则绑定于选定的 VLAN

- 管理方式：定义已定义规则的管理方式。使用该访问配置文件的用户可通过所指定的管理方式对设备进行访问。可选择的管理方式有：
  - 全部：指定该规则可以使用所有的管理方式
  - Telnet：指定该规则使用 Telnet 管理方式。若选择该方式，使用 Telnet 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝
  - Secure Telnet（SSH）：指定该规则使用 SSH 管理方式。若选择该方式，使用 Telnet 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝
  - HTTP：指定该规则使用 HTTP 管理方式。使用 HTTP 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝
  - Secure HTTPS：指定该规则使用 HTTPS 管理方式。使用 HTTPS 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝
  - SNMP：指定该规则使用 SNMP 管理方式。使用 SNMP 方式且符合访问配置文件条件的用户对于设备的访问将被允许或拒绝
- 源 IP 地址：指定已定义访问配置文件使用的接口源 IP 地址。且源 IP 地址可以是子网的 IP 地址。
- 前缀长度：指定源 IP 地址前缀或网络掩码的位数。
- 操作：定义访问规则所采用的动作。可选择：
  - 允许：允许对设备的访问。
  - 拒绝：拒绝对设备的访问。此为缺省值。
- 删除：从选定的访问配置文件中删除规则。可选择：
  - 选中：从访问配置文件中删除选定的规则。
  - 不选中：保留访问配置文件所绑定的规则。

3. 点击“创建”，打开添加配置文件规则页面：

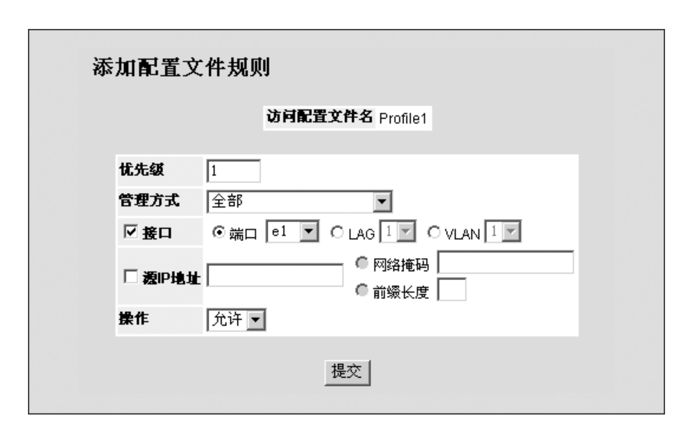


图 5-4 添加配置文件规则页面

4. 定义各字段。

5. 点击“提交”将配置规则添加至访问配置文件并更新系统。

修改配置文件规则：

1. 点击：安全>管理安全>认证>配置文件规则，打开配置文件规则页面。

2. 点击✎，打开配置文件规则设置页面：

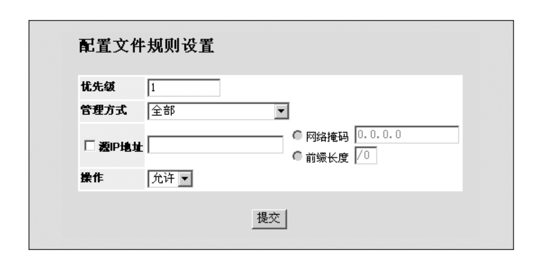


图 5-5 配置文件规则设置页面

3. 修改相应字段。

4. 点击“提交”，修改配置文件规则并更新系统。

5.1.1.3 定义认证配置文件

认证配置文件允许网络管理员可以指定用户认证的认证方式。依照所定义的多个认证方式顺序，认证本身可以在本地或远程服务器上进行。如果第一种认证方式不可用，则会使用下一种方式。例如，选择的认证方式为 RADIUS 和“本地”，当 RADIUS 服务器不可用时，则将会在本地对用户进行认证。

定义认证配置文件：

1. 点击：安全>管理安全>认证>认证配置文件，打开认证配置文件页面：



图 5-6 认证配置文件页面

认证配置文件页面提供了如下表格：

➢ 登录认证配置文件

➢ 启用认证配置文件

每张表格包含下列选项：

➢ 配置文件名：包含一张已添加的用户定义的认证配置文件。

➢ 方法：定义了用户认证的方式。可选择：

– None：指定当前认证配置文件不使用认证。

– Local：在交换机上对用户进行认证。交换机对用户名和密码进行检查认证。

– RADIUS：在 RADIUS 服务器上对用户进行认证。更多相关信息，参见“RADIUS 服务器设置”

– Line：使用“线路密码”对用户进行认证

– Enable：使用“启用密码”对用户进行认证

➢ 删除：删除选定的认证配置文件。可选择：

– 选中：删除选定的认证配置文件

– 不选中：保留认证配置文件

2. 点击“创建”，打开添加认证配置文件页面。



图 5-7 添加认证配置文件页面

3. 选择配置文件方法并输入配置文件名。

4. 选择认证方法并点击。

5. 点击“提交”，定义认证配置文件并更新系统。

欲修改认证配置文件：

1. 点击：安全>管理安全>认证>认证配置文件，打开认证配置文件页面。

2. 点击 ，打开认证配置文件设置页面。



图 5-8 认证配置文件设置页面

3. 选择认证方法并点击 。

4. 点击“提交”，选定认证方式并更新系统。

5.1.1.4 映射认证配置文件

已定义的认证配置文件可以用以对访问方式进行管理。例如，控制台用户可以通过认证配置文件列表 1 被认证，而 Telnet 用户则可以通过认证配置文件列表 2 进行认证。使用箭头对认证方式进行选择。选择认证方式的顺序即是认证方式的使用 顺序。

映射认证方式：

1. 点击：安全>管理安全>认证>认证映射，打开认证映射页面：



图 5-9 认证映射页面

认证映射页面包含以下字段：

➢ 终端：表示认证配置文件用来认证终端用户。

- Telnet：表示认证配置文件用来认证 Telnet 用户。
- Secure Telnet（SSH）：表示认证配置文件用来认证 Secure Shell（SSH）用户。SSH 提供到设备的客户安全和加密的远端连接。
- Secure HTTP：表示认证方法用于 Secure HTTP 访问。可能的值是：
  - None：表示没有用于访问的认证方法。
  - Local：表示认证发生在本地。
  - RADIUS：表示认证发生在 RADIUS 服务器。
  - Local，RADIUS：表示认证首先发生在本地。如果本地不能检验认证，RADIUS 服务器将认证管理方式。如果 RADIUS 服务器不能认证管理方式，则会话被锁定。
  - RADIUS，Local：表示认证首先发生在 RADIUS 服务器。如果不能在 RADIUS 服务器检验认证，会话将在本地认证。如果本地不能认证会话，则会话被锁定。
  - Local，RADIUS，None：表示认证首先发生在本地。如果本地不能检验认证，RADIUS 服务器将认证管理方式。如果 RADIUS 服务器不能认证管理方式，则会话被许可。
  - RADIUS，Local，None：表示认证首先发生在 RADIUS 服务器。如果 RADIUS 服务器不能检验认证，会话将在本地认证。如果本地不能认证会话，则会话被许可。
- HTTP：表示认证方法用于 HTTP 访问。可能的值是：
  - None：表示没用认证方法被用于访问。
  - Local：表示认证发生在本地。
  - RADIUS：表示认证发生在 RADIUS 服务器。
  - Local，RADIUS：表示认证首先发生在本地。如果本地不能检验认证，

RADIUS 服务器将认证管理方式。如果 RADIUS 服务器不能认证管理方式，则会话被锁定。

  - RADIUS，Local：表示认证首先发生在 RADIUS 服务器。如果 RADIUS 服务器不能检验认证，会话将在本地认证。如果本地不能认证会话，则会话被锁定。
  - Local，RADIUS，None：表示认证首先发生在本地。如果本地不能检验认证，RADIUS 服务器将认证管理方式。如果 RADIUS 服务器不能认证管理方式，则会话被许可。
  - RADIUS，Local，None：表示认证首先发生在 RADIUS 服务器。如果 RADIUS 服务器不能检验认证，会话就在本地认证。如果本地不能认证会话，则会话被许可。

2. 设定终端、Telnet、Secure Telnet（SSH）各字段值。
3. 在 Secure HTTP 选择框中映射相应的认证方式。

4. 在 HTTP 选择框中映射相应的认证方式。

5. 点击“提交”，保存认证映射并更新系统。

5.1.1.5 TACACS+主机设置

终端访问控制器控制系统(TACACS+)提供了集中的用户访问安全验证。本系统共支持 4 个 TACACS+服务器。

TACACS+提供了一个集中的用户管理系统，同时保持了与 RADIUS 以及其他认证方法的连贯性。TACACS+提供了下列服务：

- 认证：在登录时通过用户名和用户定义的密码提供认证

- 授权：在登录时进行。一旦完成认证会话，就使用已认证的用户名开始授权会话。

TACACS+协议通过在客户端和服务器之间使用加密协议进行数据交换来确保网络的完整性。

☞ 注意：

TACACS+缺省参数为用户指定的缺省值。缺省设置将被应用至新定义的TACACS+服务器。若未定义缺省值，则将系统缺省值应用至新的TACACS+服务器。

定义 TACACS+认证设置：

1. 点击：安全>管理安全>认证>TACACS+，打开 TACACS+页面：



图 5-10 TACACS+页面

默认参数部分包含以下字段：

- 源 IP 地址：定义用于在设备和 TACACS+服务器之间的会话的设备源 IP 地址。

- 密钥字符串：为在设备和 TACACS+服务器间的 TACACS+通信定义认证和加密密钥。密钥必须与用在 TACACS+服务器上的密码匹配。

- 应答超时：定义在设备和 TACACS+之间的连接超时前经过的默认时间。默认值 5。

TACACS+页面也包含以下字段：

- 主机 IP 地址：定义 TACACS+服务器 IP 地址。
- 优先级：使用 TACACS+服务器的顺序。该值范围是 0-65535。默认是 0。
- 源 IP 地址：定义用于在设备和 TACACS+服务器间的会话的设备源 IP 地址。
- 认证端口：定义发生 TACACS+会话的端口号。
- 应答超时：定义在设备和 TACACS+之间的连接超时前经过的时间数（秒）。该值范围是 1-1000 秒。
- 单连接：在设备和 TACACS+服务器间维持单个开放连接。可能的值是：
  - 选中：启用单个连接。
  - 不选中：禁用单个连接。
- 状态：表示在设备和 TACACS+服务器间的连接的状态。可能的值是：
  - 连接：表示在设备和 TACACS+服务器间当前有一个连接。
  - 未连接：表示在设备和 TACACS+服务器间当前没有连接。
- 删除：删除 TACACS+服务器。可能的值是：
  - 选中：删除选择的 TACACS+服务器。
  - 不选中：维持 TACACS+服务器。

2. 点击“创建”，打开添加 TACACS 主机页面：



图 5-11 添加 TACACS 主机页面

定义各字段。

3. 点击“提交”，以定义 TACACS 主机并更新系统。

修改 TACACS+服务器设置：

1. 点击：安全>管理安全>认证>TACACS+，打开 TACACS+页面。
2. 选择 TACACS+服务器条目。

3. 点击 ，打开 TACACS 主机设置页面：

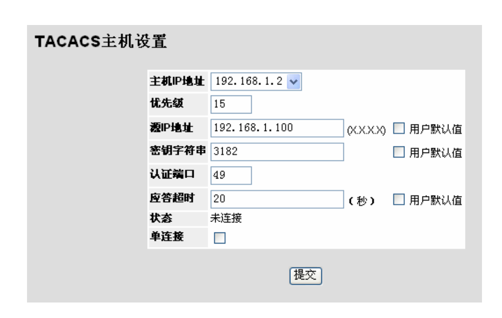


图 5-12 TACACS 主机设置页面

4. 修改参数。

5. 点击“提交”，保存 TACACS 主机设置并更新系统。

5.1.1.6 RADIUS服务器设置

远程认证拨号用户服务（RADIUS）服务器为网络提供了额外的安全。RADIUS 服务器为 WEB 访问提供了集中的认证方式。

所有缺省参数均是用户自定义的，并被应用至新定义的 RADIUS 服务器中。若新的缺省参数未被定义，则系统缺省值将被应用至新定义的 RADIUS 服务器中。

定义 RADIUS 服务器：

1. 点击：安全>管理安全>认证>RADIUS，打开 RADIUS 页面：



图 5-13 RADIUS 页面

RADIUS 页面的默认参数部分包含以下字段：

➢ 默认条目：定义在发生失败前被发送到 RADIUS 服务器的传输请求数。可能的值是 1-10。默认值是 3。

➢ 默认应答超时：定义在重新尝试查询前设备等待来自 RADIUS 服务器的应答或切换到另一服务器的时间数（秒）。可能的值是 1-30。默认值是 3。

- 默认停用时间：定义 RADIUS 服务器忽略服务请求的默认时间数（分钟）。范围是 0-2000。默认值是 0。
- 默认密钥：定义用于认证和加密所有在设备和 RADIUS 服务器之间的 RADIUS 通信的默认密钥。密钥必须匹配 RADIUS 密码。
- 源 IP 地址：定义访问 RADIUS 服务器的设备的默认 IP 地址。

RADIUS 页面也包含以下字段：

- IP 地址：列出 RADIUS 服务器的 IP 地址。
- 优先级：显示 RADIUS 服务器优先级。可能的值是 1-65535，1 是最高优先级值。RADIUS 服务器优先级用来配置服务器查询顺序。
- 认证端口：标志认证端口。认证端口用来检验 RADIUS 服认证。认证端口默认是 1812。
- 条目号：定义在发生失败前被发送到 RADIUS 服务器的传输请求数。可能的值是 1-10。默认值是 3。
- 应答超时：定义在重试查询前设备等待来自 RADIUS 服务器的应答或切换到另一服务器的时间数（秒）。可能的值是 1-30。默认值是 3。
- 停用时间：定义 RADIUS 服务器忽略服务请求的默认时间数（分钟）。范围是 0-2000。默认值是 0。
- 源 IP 地址：定义访问 RADIUS 服务器的设备的默认 IP 地址。
- 使用类型：指定 RADIUS 服务器认证类型。默认值是全部。可能的值是：
  - 登录：表示 RADIUS 服务器用来认证用户名和口令。
  - 802.1X：表示 RADIUS 服务器用于 802.1X 认证。
  - 全部：表示 RADIUS 服务器用来认证用户名和口令以及 802.1X 端口认证。
- 删除：删除 RADIUS 服务器。可能的值是：
  - 选中：删除选择的 RADIUS 服务器。
  - 不选中：维持 RADIUS 服务器。这是默认值。

2. 点击“创建”，以打开添加 RADIUS 服务器页面：

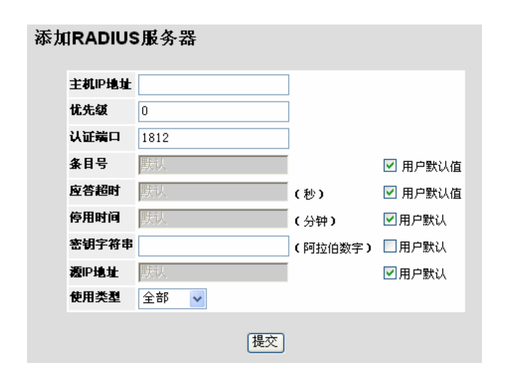


图 5-14 添加 RADIUS 服务器页面

3. 定义各字段。

4. 点击“提交”，添加 RADIUS 服务器并更新系统。

修改 RADIUS 服务器设置：

1. 点击✎，打开 RADIUS 服务器设置页面：

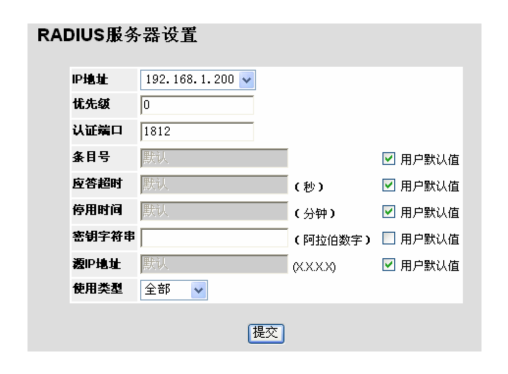


图 5-15 RADIUS 服务器设置页面

2. 修改各字段。

3. 点击“提交”，以保存 RADIUS 服务器设置并更新系统。

5.1.2 密码配置

此部分包含了定义密码的相关信息，并包含了如下主题：

➢ 定本地用户

➢ 设定连接密码

➢ 设定启用密码

5.1.2.1 设定本地用户

网络管理员可以通过本地用户页面对用户、密码和访问级别加以设定。

设定本地用户：

1. 点击：安全>管理安全>密码>本地用户，进入本地用户页面：



图 5-16 本地用户页面

本地用户页面包含以下字段：

- 用户名：显示用户的名称。
- 访问级别：显示用户的访问级别，最低的访问级别是 1 最高的是 15。15 级访问级别的用户是特权用户。
- 锁闭状态：显示用户状态。
- 删除：从用户名列表里将用户删除，可能的值包括：
  - 选中：删除选择的本地用户。
  - 不选中：保留本地用户。

2. 点击“创建”，进入添加本地用户页面：



图 5-17 添加本地用户页面

除本地用户页面所包含的字段外，添加本地用户页面包含以下字段：

- 密码：设定本地用户的密码。最多可包含 159 个字符。
- 确认密码：对密码进行验证。

3. 设定各字段
4. 点击“提交”，以保存本地用户密码并更新系统。

5.1.2.2 设定连接密码

网络管理员可以在连接密码页面对连接密码进行设定。设定连接密码之后，可将特定的管理方式分配给该密码。可以通过以下几种方式对设备进行访问：

- 控制台密码
- Telnet 密码
- 安全 Telnet 密码

对连接密码进行配置：

1. 点击：安全> 管理安全> 密码> 线路密码，进入连接密码页面：



图 5-18 连接密码页面

连接密码页面包含以下字段：

- 控制台连接密码：设定通过控制台会话访问该设备的连接密码，密码最多可包含 159 个字符。
- Telnet 连接密码：设定通过 Telnet 会话访问该设备的连接密码，密码最多可包含 159 个字符。
- 安全 Telnet 连接密码：设定通过 Secure Telnet 会话访问该设备的连接密码，密码最多可包含 159 个字符。
- 密码确认：确认所设定的连接密码。密码以*****格式显示。

2. 设定控制台连接密码、Telnet 连接密码和安全 Telnet 连接密码参数。
3. 重新设定上一步所输入的每一个密码以进行验证。
4. 点击“提交”，配置连接密码并更新系统。

5.1.2.3 设定启用密码

启用密码页面为特定的访问级别设置一个本地密码。

对启用密码进行配置：

1. 点击：安全>管理安全>密码>启用密码，进入启用密码页面：



图 5-19 启用密码页面

启用密码页面包含以下字段：

- 级别：设定与启用密码相关联的访问级别。取值范围为 1-15。
- 密码：设定启用密码。
- 确认密码：对新的启用密码加以确认。密码以******格式出现。

2. 配置各参数并点击“提交”，启用密码并更新系统。

5.2 网络安全配置

网络安全包括访问控制列表和端口锁定。该部分包含以下主题：

- 网络安全概述
- 定义网络认证属性
- 配置流量控制

5.2.1 网络安全概述

该部分包含网络安全的概述，并包含以下主题：

- 基于端口的认证
- 基于端口的高级认证

5.2.1.1 基于端口的认证

基于端口的认证通过外部服务器对每个端口的用户进行认证。只用通过认证允许的系统用户方能传输和接收数据。所有端口通过在 RADIUS 服务器上使用扩展认证协议(EAP)进行认证。

端口认证包括：

- 认证者：指在允许对系统进行访问之前被认证的设备端口。
- 恳请方：指连接至被认证端口请求访问系统服务的主机。
- 认证服务器：指为认证者进行认证并指示恳请方是否被授权访问系统服务。

基于端口的认证创建了两种访问状态：

- 受控访问：若恳请方被授权，允许恳请方与系统之间的通信。
- 未受控访问：允许未受控的通信而不受端口状态的限制。

5.2.1.2 基于端口的高级认证

基于端口的高级认证使得多个主机可以被绑定至单个端口。基于端口的高级认证仅需要一台主机被认证所有的主机就可访问系统。若端口未被认证，则所连接的所有主机将无法访问网络。

基于端口的高级认证同时支持基于用户的认证。通常可以在设备中定义 VLAN，即使所指定的端口所绑定的 VLAN 是未被授权的。例如，VoIP 并不需要认证，而数据流则需要。可以对不需要进行

认证的 VLAN 进行定义。未认证的 VLAN 对于用户是可用的，即使绑定到该 VLAN 的端口被设定为已认证。

基于端口的高级认证通过以下模式实现：

- 单主机模式：仅允许已认证的主机对端口的访问。
- 多主机模式：单个端口可连接多台主机。所有访问网络的主机中仅需要一台被认证。若该主机认证失败，或接收到 EAP-logoff 信息，则所有连接主机对网络的访问都将被拒绝。
- 来宾 VLAN：限制已认证端口的网络访问。若某端口被基于端口认证拒绝网络访问，而来宾 VLAN 被启用，该端口可以接受有限的网络服务。例如，网络管理员可以使用基于端口认证的来宾 VLAN 拒绝用户对网络的访问，但可以保证其对 Internet 的访问。
- 未认证 VLAN：即使被捆绑到 VLAN 的所有端口均被设定为未认证，网络仍然可用。

5.2.2 定义网络认证属性

网络安全认证属性允许网络管理者对网络认证参数进行配置。此外，可在网络安全认证属性页面启用来宾 VLAN。

定义网络认证属性：

1. 点击：安全>网络安全>认证>属性，进入系统信息页面：



图 5-20 系统信息页面

系统信息页面包含以下字段：

- 基于端口的认证状态：指明是否在设备上启用了端口认证。可能的值包括：
  - 启用：启用基于端口的认证。
  - 禁用：禁用基于端口的认证。
- 认证方法：指定端口认证的认证方式。可能的值包括：
  - 无：指明没有对端口进行认证。
  - RADIUS：使用 RADIUS 服务器对端口进行认证。

– RADIUS，无：首先使用 RADIUS 服务器认证。如果端口没有被认证，就使用无认证，会话将被允许。

➢ 来宾 VLAN：指定是否开启来宾 VLAN。可能的值包括：

  – 启用：对未授权的端口启用来宾 VLAN。如果启用了来宾 VLAN，没有被授权的端口将自动加入到在 VLAN 列表中选择的 VLAN。

  – 禁用：禁用基于端口的认证，这是默认配置。

2. 启用基于端口的认证状态，定义认证方法，启用来宾 VLAN 并选择 VLAN 列表。

3. 点击“提交”，保存网络安全认证属性并更新系统。

5.2.2.1 定义端口认证属性

端口认证页面允许网络管理者对基于端口认证的全局参数进行配置。

定义基于端口认证的全局属性：

1. 点击：安全>网络安全>认证>端口认证，进入端口认证页面：



图 5-21 端口认证页面

端口认证页面包含以下字段：

➢ 从条目号：从选择的条目复制端口认证信息。

➢ 复制到条目号：把端口认证信息复制到选择的条目。

➢ 端口：显示启用基于端口认证的接口列表。

➢ 用户名：显示使用者的用户名。

➢ 当前端口控制：显示当前端口认证状态，可能的值包括：

  – 自动：启用基于端口的认证。接口基于设备和客户端的认证情况在授权与被授权之间变化。

– 授权：指明一个接口不需要认证即处在授权状态。接口不需要客户端通过基于端口的认证就能够接受和发送数据。

– 未授权：拒绝选择的端口在未授权的状态下访问。这个设备不能通过这个接口对客户端提供授权服务。

➢ 启用定期重新认证：允许立即端口重认证。可能的值包括：

– 启用：启用立即端口重认证，这是默认值。

– 禁用：禁用端口重认证。

➢ 定期重新认证：显示所选的端口重认证间隔的时间。以秒为单位。默认值是 3600 秒。

➢ 认证状态：显示当前的认证状态。

➢ 无提示时段：显示当认证改变后保持不提示的时长，单位是秒。取值范围是 0 - 65535，默认的值是 60 秒。

➢ 重发 EAP：定义重新发送 EAP 的时间，单位是秒。默认值是 30 秒。

➢ 最大 EAP 请求：显示发送 EAP 请求的总数。如果在定义的时间内没有收到响应，认证过程将被重启。默认值是 2 次。

➢ 申请方超时：显示重新发送 EAP 请求的时长。默认值是 30 秒。

➢ 服务器超时：显示对认证服务器重新发送认证请求的时间。默认值是 30 秒。

➢ 终止原因：指明端口认证终止的原因。

2. 点击，进入端口认证设置页面：



图 5-22 端口认证设置页面

3. 定义各字段。

– 选中“开始重新认证”复选框，在提交时立即对所选端口进行重新认证。

4. 点击“提交”，保存端口认证设置并更新系统。

5.2.2.2 配置多台主机

多台主机页面允许网络管理者对特定的端口和 VLAN 配置基于端口认证的高级设置。欲了解端口认证的更多高级信息，参见高级端口认证。

定义网络认证的全局属性：

1. 点击：安全>网络安全>认证>多台主机，进入多台主机页面：



图 5-23 多台主机页面

多台主机页面包含以下字段：

- 端口：显示启用高级基于端口认证的端口。
- 多台主机：指明是否启用多台主机。多台主机必须在关闭进入过滤和打开端口锁定安全的情况下才能起用。可能的值包括：
  - 多台主机：启用多台主机。
  - 禁用：禁用多台主机。
- 侵入时措施：定义在单主机模式时收到一个非请求者的数据包时的措施。
  - 传输：传输数据包。
  - 丢弃：丢弃数据包，这是默认值。
  - 关闭：丢弃数据包然后关闭端口，断口保持关闭一直到激活或者设备复位。
- 陷阱：指明是否启用多台主机的陷阱。可能的值包括：
  - 是：指明启用多台主机陷阱。
  - 否：禁用多台主机陷阱。

➢ 陷阱频率：定义陷阱发送间隔。陷阱频率的取值范围是（1 - 1000000）。默认值是 10 秒。

➢ 状态：指明主机状态，如果这里是一个星号（*），这个端口没有连接或者是已经关闭，可能的值包括：

– 未授权：指明这个端口控制被指向未授权而且端口连接断开。或者端口控制是自动，但是客户端没有通过这个端口的认证。

– 非自动模式：指明端口控制被指向认证而且客户端拥有访问权限。

– 单主机锁定：指明端口控制是自动而且单个客户端通过这个端口认证。

– 非单主机：指明多主机被启用。

➢ 侵入数目：指明非请求者 MAC 地址的包在单主机模式下到达接口的数量。

2. 点击✎，进入多台主机设置页面：

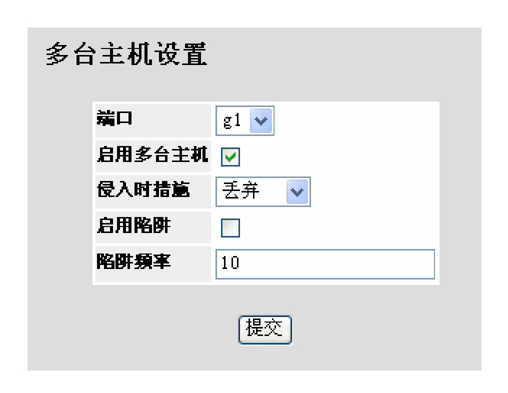


图 5-24 多台主机设置页面

3. 定义各字段。

4. 点击“提交”，保存多台主机设置并更新系统。

5.2.2.3 定义认证主机

认证主机页面包含了已认证用户的列表。

定义认证主机：

1. 点击：安全>网络安全>认证>已认证主机，进入认证主机页面：



图 5-25 认证主机页面

认证主机页面包含以下字段：

- 用户名：显示经过认证且被允许的请求者。
- 端口：显示端口号。
- 会话时间：显示请求者已登陆的时间。
- 认证方法：显示最后一条会话所使用的认证方式，可能的值包括：
  - 无：指明端口没有使用认证。
  - RADIUS：使用 RADIUS 服务器进行认证。
  - RADIUS，无：首先使用 RADIUS 服务器认证。如果端口没有被认证，就使用无认证方法，会话将被允许。
- MAC 地址：显示请求者的 MAC 地址。

5.2.3 配置流量控制

该部分同时包含了端口安全和风暴控制的管理信息，包括以下主题：

- 管理端口安全
- 启用风暴控制

5.2.3.1 管理端口安全

可以通过限制使用特定 MAC 地址的用户对特定端口的访问来增加网络安全。这些 MAC 地址可以是动态学习或静态配置的。锁定的端口安全同时对接收到的数据包和特定端口接收到的已学习的数据包进行监控。仅限于使用特定 MAC 地址的用户对锁定端口的访问。这些地址要么是手动定义的，要么是动态学习到的。当一个锁定端口接收到一个数据包，且带有 TP-LINK 源 MAC 地址的数据包未被绑定于该端口（该地址可能被学习到别的端口，或该地址对于系统是未知的），此时保护机制将被激活并提供各种选项。

对于到达锁定端口的未经授权的数据包将：

- 转发
- 丢弃
- 丢弃并发送陷阱
- 关闭该端口

锁定端口安全同时在配置文件中存储了一张 MAC 地址表。这个地址表可以在设备重启后恢复。

可以在端口安全页面激活被禁用的端口。

查看端口安全参数：

1. 点击：安全>网络安全>通信控制>端口安全，进入端口安全页面：



图 5-26 端口安全页面

端口安全页面包含了以下字段：

➢ 接口：显示端口或者 LAG 名称。

➢ 接口状态：指明主机状态，可能的值包括：

  – 未授权：指明端口控制被强制未授权。端口连接中断或者端口控制设置为自动，但是客户端没有通过端口的认证。

  – 非自动模式：指明端口控制指向授权，客户端拥有完全的访问权。

  – 单主机锁定：指明端口控制设为自动，单个的客户端通过端口的认证。

➢ 记忆模式：指明锁定端口的类型。记忆模式只能在设置端口选择了锁定后才能被启用。可能的值包括：

  – 标准锁定：使用标准锁定方式对端口进行锁定。端口立即被锁定，不管端口已经学习了多少地址。

  – 限制动态锁定：锁定端口并删除现在的动态地址表。端口重新学习允许的最大数量的地址。MAC 地址学习和老化都被打开。

➢ 最大条目：指定的在端口上能够学习的 MAC 地址的数量。只能在选择了锁定端口之后才能设置最大条目。另外，也要选定限制动态锁定。默认值是 1。

➢ 操作：指明在锁定端口上对接收到的数据包所作的操作。可能的值包括：

  – 转发：转发从未知源发送的数据包，不学习其 MAC 地址。

  – 丢弃：丢弃从任何未被学习的源地址发送的包，这是默认值。

  – 关闭：丢弃从任何未被学习的源地址发送的包并关闭端口。端口保持关闭直到被重新激活或者设备重启

➢ 陷阱：启用一个陷阱当锁定端口接收到一个数据包。可能的值包括：

  – 选中：启用陷阱。

– 不选中：禁用陷阱。

➢ 陷阱频率（秒）：两个陷阱之间的间隔时间。默认值是 10 秒。

欲修改接口表设置：

1. 点击✎，进入接口表设置页面：



图 5-27 接口表设置页面

2. 修改接口表设置参数。

3. 点击“提交”，保存接口表设置参数并更新系统。

5.2.3.2 启用风暴控制

风暴控制能限制设备能接受和转发的组播和广播帧数量。当 2 层数据帧被转发，广播和组播帧被泛洪至相关 VLAN 的所有端口。这样会占用带宽并加重所有端口的负载。

广播风暴是一个端口同时向网络中发送过量的广播信息所导致的结果。被转发的信息堆积在网络中，耗用网络资源导致网络超时。可通过设定数据包类型和发送速率启用千兆端口的风暴控制。系统将对进入每个端口的广播和组播帧进行单独的测量，并丢弃所有超过用户设定速率的帧。风暴控制页面提供了配置广播风暴控制的各种选项。

启用端口的风暴控制：

1. 点击：安全>网络安全>通信控制>风暴控制，进入风暴控制页面：



图 5-28 风暴控制页面

风暴控制页面包含以下字段：

➢ 端口：指明启用了风暴控制的端口。

➢ 启用广播控制：指明是否启用启用广播包控制。

– 已启用：启用选择端口的风暴控制。

– 已禁用：禁用选择端口的风暴控制。

➢ 广播模式

➢ 广播速率限制：指明对于未知包的最大转发率（千字节每秒）。对于百兆以太网口这个速率是范围是 70-100000，对于千兆以太网接口是 3500-1000000，默认值是 3500。

2. 点击✎，进入风暴控制设置页面：



图 5-29 风暴控制设置页面

3. 选中启用广播控制复选框，定义广播速率限制。

4. 点击“提交”，启用选定端口的风暴控制。

第6章　　定义IP地址

本章提供了使用 DHCP 和 ARP 设定 IP 地址，以及如何设定缺省网关和域名服务器参数等相关信息。

本章包含以下主题：

- 定义 IP 地址
- 定义域名系统

6.1　定义IP地址

该部分提供了接口 IP 地址和缺省网关，设定接口 ARP 和 DHCP 参数等信息。

该部分包含以下主题：

- 定义 IP 地址
- 定义默认网关
- 定义 DHCP 地址
- 定义 ARP

6.1.1　定义IP地址

IP 接口页面包含了 IP 地址设定参数。当帧被发往远程网络时数据包将被转发至缺省 IP。所配置的 IP 地址必须与 IP 接口同属于一个 IP 子网。

1. 点击：系统信息>IP 配置>IP 定址>IP 接口，进入 IP 接口页面：



图 6-1 IP 接口页面

IP 接口页面包含以下字段：

- IP 地址：显示当前配置的 IP 地址。

- 网络掩码：显示当前配置的 IP 地址的网络掩码。
- 接口：显示用于管理设备的接口。
- 类型：显示 IP 地址是静态的还是动态的。
  - 静态：显示该 IP 地址是一个静态 IP 地址。
  - 动态 ：显示该 IP 地址是个动态创建的 IP 地址。
- 删除：从接口删除选中的 IP 地址。可能的值是：
  - 选中：从接口删除 IP 地址。
  - 不选中：维持分配给接口的 IP 地址。

2. 点击“创建”，进入添加 IP 接口页面：



图 6-2 添加 IP 接口页面

3. 设定源 IP 地址、网络掩码、前缀长度和接口(端口、LAG 或 VLAN)
4. 点击“提交”，添加新接口并更新系统。

修改 IP 接口设置：

1. 点击：系统信息>IP 配置>IP 定址>IP 接口，进入 IP 接口页面。
2. 点击，进入 IP 接口设置页面：



图 6-3 IP 接口设置页面

3. 修改 IP 地址和接口参数
4. 点击“提交”，接口被修改并更新系统。

6.1.2 定义默认网关

当帧通过默认网关被发送到远程网络时数据包将被转发至缺省 IP。所配置的 IP 地址必须与 IP 接口同属于一个 IP 子网。

定义系统的默认网关：

1. 点击：系统信息>IP 配置>IP 定址>默认网关，进入默认网关页面：



图 6-4 默认网关页面

默认网关页面包含以下字段：

- 用户定义默认网关：表示当前默认网关的名称
- 当前默认网关：表示所定义的默认网关当前被启用
- 删除用户定义：删除所定义的默认网关

2. 输入用户定义默认网关名称。

3. 点击“提交”，网关被保存并更新系统。

6.1.3 定义DHCP地址

动态主机配置协议(DHCP)用来对网络中的设备动态分配 IP 地址。DHCP 确保所有的设备使用不同的 IP 地址而无论设备何时接入到网络中。

定义 DHCP 地址：

1. 点击：系统信息>IP 配置>IP 定址>DHCP，进入 DHCP 页面：



图 6-5 DHCP 页面

DHCP 页面包含了以下字段：

- 接口：显示连接到 DHCP 服务器的接口的 IP 地址。
- 主机名称：显示系统名称。
- 删除：删除 DHCP 接口。可能的值是：
  - 选中：删除选中的 DHCP 接口。
  - 不选中：维持 DHCP 接口。

2. 点击“创建”，进入添加 DHCP IP 接口页面：



图 6-6 添加 DHCP IP 接口页面

3. 选择接口。
4. 输入主机名称。
5. 点击“提交”，新接口被添加至 DHCP 并更新系统。

删除 DHCP 设定：

- 点击删除复选框。当前 DHCP 设定被删除，系统被更新。

6.1.4 设定ARP

地址解析协议将 IP 地址转换成物理地址，并将 IP 地址映射成 MAC 地址。ARP 使得在仅已知相邻主机 IP 地址的情况下就允许对该主机通信。

设定 ARP：

1. 点击：系统信息>IP 配置>IP 定址>ARP，进入 ARP 页面：



图 6-7 ARP 页面

ARP 页面包含以下字段：

- ➢ ARP 条目老化：指定通过 ARP 表条目的老化时间数（秒）。在 ARP 条目老化时间过后，该条目将从表中删除。范围是 1 - 40000000，默认值是 60000 秒。
- ➢ 清除 ARP 表条目：指定被清除的 ARP 条目的类型。可能的值是：
  - – 无：维持 ARP 条目。
  - – 全部：清除所有 ARP 条目。
  - – 动态：只清除动态 ARP 条目。
  - – 静态：只清除静态 ARP 条目。
- ➢ 接口：显示 ARP 参数的接口类型，可能的值是：
  - – 端口：表示定义 ARP 参数的端口。
  - – LAG：表示定义 ARP 参数的 ALG。
  - – VLAN：表示定义 ARP 参数的 VLAN。
- ➢ IP 地址：表示工作站 IP 地址，与填在其下的 MAC 地址相关联。
- ➢ MAC 地址：显示工作站 MAC 地址，其在 ARP 表中与 IP 地址相关联。
- ➢ 状态：显示 ARP 表条目类型。可能的值是：
  - – 动态：表示 ARP 条目是动态学习到的。
  - – 静态：表示 ARP 条目是一静态条目。
- ➢ 删除：删除指定的 ARP 条目。可能的值是：
  - – 选中：删除选中的 ARP 条目。

– 不选中：维持当前 ARP 条目。

2. 定义 ARP 表项的老化时间。

3. 定义清除 ARP 表条目的参数。

4. 点击“创建”，进入 ARP 设置页面。



图 6-8 ARP 设置页面

5. 选择接口（端口、LAG 或 VLAN）。

6. 设定 IP 地址和 MAC 地址。

7. 点击“提交”，新表项被添加至 ARP 中并更新系统。

6.2 定义域名系统

域名系统将用户定义的域名转换成IP地址。一旦域名被分配，DNS服务器将其名称解析成数字的IP地址。例如，www.ipexample.com被解析成 192.87.56.2。DNS服务器本身维护一个域名和对应IP地址的数据库。

这部分包含以下主题：

- 定义 DNS 服务器
- 配置主机映射

6.2.1 定义DNS服务器

DNS 服务器页面包含启用和激活特定 DNS 服务器的选项。

启用并定义 DNS 服务器：

1. 点击：系统信息>IP 配置>动态域名系统>DNS 服务器，进入 DNS 服务器页面：



图 6-9 DNS 服务器页面

DNS 服务器页面包含以下字段：

- 启用 DNS：启用翻译 DNS 名称为 IP 地址。可能的值是：
  - 选中：把域名转换 IP 地址。
  - 不选中：禁用域名到 IP 地址的转换。
- 默认域名：指定用户定义的 DNS 服务器名称。
- 类型：显示 IP 地址类型。可能的值是：
  - 动态：IP 地址是动态获得的地址。
  - 静态：IP 地址是静态地址。
- DNS 服务器：显示 DNS 服务器 IP 地址。在添加 DNS 服务器页面中添加 DNS 服务器。
- 活动服务器：指定 DNS 服务器为当前活动状态。可能的值是：
  - 选中：使激活选中的 DNS 服务器在设备重启后生效。
  - 不选中：使选中的 DNS 服务器在设备重启后失效。这是默认值。

2. 选中启用 DNS 复选框。
3. 设定默认域名。
4. 点击“创建”，进入添加 DNS 服务器页面：

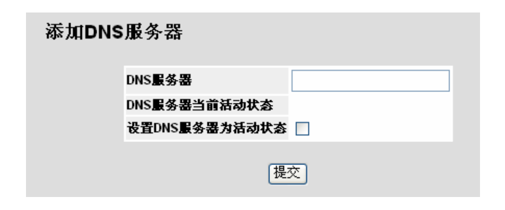


图 6-10 添加 DNS 服务器页面

5. 输入 DNS 服务器名称并选中设置 DNS 服务器为活动状态复选框。

6. 点击“提交”，新服务器被添加并更新系统。

6.2.2 配置主机映射

DNS 主机映射页面提供定义 DNS 主机映射的信息。

定义主机映射：

1. 点击：系统信息 > IP 配置 > 动态域名系统 > 主机映射。打开主机映射页面：



图 6-11 主机映射页面

主机映射页面包含以下字段：

- 主机名称：显示用户定义的默认域名。已定义的默认域名被应用给所有无 资格的主机名称。主机名称可以包含最多 158 个字符。
- IP 地址：显示 DNS 主机 IP 地址。
- 删除：删除默认域名。可能的值是：
  - 选中：删除选中的 DNS 主机。
  - 不选中：维持当前 DNS 主机映射表。

2. 点击“创建”，打开添加 DNS 主机页面：

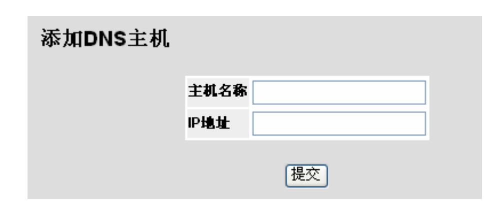


图 6-12 添加 DNS 主机页面

3. 填入主机名称和 IP 地址。

4. 点击“提交”，添加新的主机到主机映射页面中的主机列表中。

第7章　　接口配置

这个部分包含下列主题：

➢ 配置端口

➢ 配置链路聚合组（LAG）

➢ 配置 VLAN

7.1　配置端口

这个配置页包含定义端口参数。

定义端口参数：

1. 点击：网桥配置>接口>接口配置，打开接口配置页面：



图 7-1 接口配置页面

接口配置页面包含以下两个部分：

➢ 端口表

➢ LAG 表

端口表包含以下字段：

➢ 接口：显示已配置的端口号。

➢ 端口类型：显示端口的类型。

➢ 端口状态：显示端口当前是否运行。可能的值是：

- 连接：显示该端口当前正在运行。
- 未连接：显示该端口当前未运行。

- 端口速率：显示为端口配置的速率。端口类型决定了端口可能的速率设置。端口速率仅当禁用了自动协商时才可以配置。可能的值是：
  - 10M：表示端口当前工作在 10Mbps。
  - 100M：表示端口当前工作在 100Mbps。
  - 1000M：表示端口当前工作在 1000Mbps。
- 双工模式：显示端口双工模式。仅当自动协商被禁止并且端口速率是 10M 或 100M 时该项目才可以配置。不能在 LAG 上配置该项目。可能的值是：
  - Full：接口支持设备和其对端连接端口间同时双向传输。
  - Half：接口支持设备和其客户间在某一时刻只能单向传输。
- 自动协商：显示在端口上的自动协商状态。自动协商是一种可以在两个连接端口间启用一个端口向另一个端口公告其传输速率，双工模式和流控能力的协议。
- 公告：定义自动协商设置端口公告。可能的值是：
  - 最大能力：表示所有端口速率和双工模式设置都是可以接收的。
  - 10 Half：表示端口公告的是 10Mbps 速率和半双工模式设置。
  - 10 Full：表示端口公告的是 10Mbps 和全双工模式设置。
  - 100 Half：表示端口公告的是 100Mbps 速率和半双工模式设置。
  - 100 Full：表示端口公告的是 100Mbps 速率和全双工模式设置。
  - 1000 Full：表示端口公告的是 1000Mbps 速率和全双工模式设置。
- 背压：显示端口的背压模式。背压模式和半双工模式一起用做禁止端口接收信息。
- 流控：显示端口的流控状态。当端口处于全双工模式时工作。
- MDI/MDIX：显示端口的 MDI/MDIX 状态。集线器和交换机协商地通过电缆连接对端终端，所以当集线器或交换机连一个终端时，可以使用直通以太网电缆且要恰当的匹配线对。当两个集线器或交换机互连时，或两个终端互连时，用交叉电缆且确保正确的线对来连接。可能的值是：
  - Auto：使用自动检测电缆类型。
  - MDI（接口相关介质）：用于终端。
  - MDIX（带交叉的接口相关介质）：用于交换机。
- LAG：表示端口是否是接口主干（LAG）的一部分。

LAG 表包含以下字段：

- LAG：表示端口是否是接口主干（LAG）的一部分。
- 说明：显示端口说明。
- LAG 类型：表示由第一个分配给 LAG 的端口定义的 LAG 类型。例如，100-Copper 或 100-Fiber。
- LAG 状态：表示 LAG 是否连接。
- LAG 速率：显示已为 LAG 配置的主干速率。可能的值是：
  - 10：表示端口当前工作在 10Mbps。
  - 100：表示端口当前工作在 100Mbps。
  - 1000：表示端口当前工作在 1000Mbps。
- 自动协商：显示 LAG 的自动协商状态。自动协商是一种可以在两个连接端口间启用一个端口向另一个端口公告其传输速率，双工模式和流控能力的协议。
- 流控：显示 LAG 的流控状态。

2. 点击该条目后的✎进行更改，打开端口或 LAG 设置页面：



图 7-2 端口配置设置页面

除了接口配置页面的一些选项外，端口配置设置页面还包含以下附加的内容：

- 重新激活端口：重新激活一个暂挂的端口，可选的值有：
  - 选中：重新激活或开启暂挂的端口。
  - 不选中：维持端口当前锁定或暂挂的状态。

3. 修改管理速率，管理双工，管理公告等字段。

4. 点击“提交”，参数被保存并更新设备。

7.2 配置链路聚合组（LAG）

链路聚合通过将一组端口链接在一起形成单个 LAG(链路聚合组)来优化端口的使用。聚合端口可以使设备之间的带宽成倍增加、增强端口灵活性并提供链路冗余。

TP-LINK 设备既支持静态 LAG，也支持链路聚合控制协议 (LACP) LAG。LACP LAG 与位于其它设备上的 LACP 端口协商聚合端口的链路。如果其它设备端口也是 LACP 端口，则设备将在设备之间建立 LAG。

聚合端口时应考虑以下因素：

- LAG 内的所有端口必须为相同的介质类型。
- 未在端口上配置 VLAN。
- 端口未分配至不同的 LAG。
- 端口上未配置自适应模式。
- 端口处于全双工模式。
- LAG 中的所有端口具有相同的入口筛选和标记模式。
- LAG 中的所有端口具有相同的背压和流控制模式。
- LAG 中的所有端口具有相同的优先级。
- LAG 中的所有端口具有相同的收发机类型。
- 设备最多支持八个 LAG，且每个 LAG 中有八个端口。
- 仅当端口不属于先前配置的 LAG 时，才可以将端口配置为 LACP 端口。
- 添加至 LAG 的端口将失去其各自的端口配置。将端口从 LAG 中删除时，原始端口配置将应用于端口。

这个部分包含下列主题：

- 定义 LAG 成员
- 配置 LACP

7.2.1 定义LAG成员

定义 LAG 成员：

1. 点击：网桥配置>接口>LAG 成员，打开接口主干配置页面：



图 7-3 接口主干配置页面

接口主干配置页面包含下列字段：

- LAG 端口：显示 LAG 序号。
- 名称：显示使用者定义的端口名称。
- 连接状态：显示连接工作状态。
- 成员：显示 LAG 配置的端口，成员组中显示粗体的是有效的，显示灰色是无效的。
- 删除：删除 LAG，可选的值有：
  - 选中：删除选定的 LAG
  - 不选中：维持这个 LAG。

修改 LAG 成员：

1、 点击✎，打开修改 LAG 成员页面：

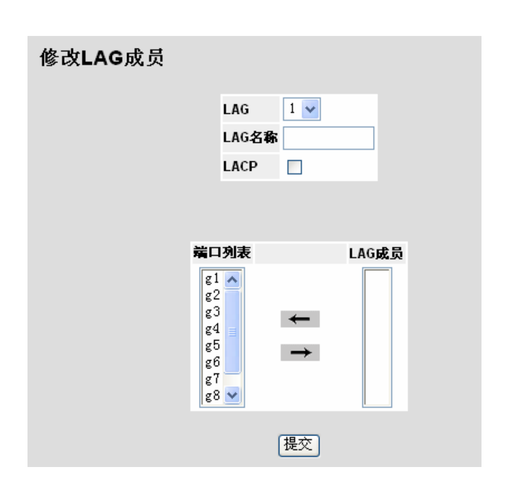


图 7-4 修改 LAG 成员页面

修改 LAG 成员页面包含以下字段：

- LAG：包含一个用户自定义的下拉 LAG 列表。
- LAG 名称：显示用户自定义的 LAG 名称
- LACP：指出 LACP 是否在 LAG 上被定义，可选的值包括：
  - 选中：在 LAG 上启用 LACP
  - 不选中：在 LAG 上禁用 LACP，这是默认的值。
- 端口列表：显示一个端口列表，端口列表中的端口可以被添加到 LAG。
- LAG 成员：显示 LAG 中包含的端口列表。

2. 为端口定义 LAG 字段。
3. 点击端口列表中的端口并添加到 LAG 成员列表中，用→。
4. 点击"提交"，接口 LAG 成员特性被修改，并更新设备。

7.2.2 配置LACP

链路聚合组(LAG)中的端口如果以同一速率运行，则可以包含不同的介质类型。通过在相关链路上启用链路聚合控制协议(LACP)，可以手动配置或自动配置聚合链路。聚合端口可以被链接至链路聚合端口组。每个组都包含具有相同速率的端口。LACP 参数页面包含用于配置 LACP LAG 的字段。

查看与配置 LACP：

1. 点击：网桥配置>接口>LACP 参数，打开接口 LACP 成员关系页面：



图 7-5 接口 LACP 成员关系页面

接口 LACP 成员关系页面包含以下字段：

➢ LACP 系统优先级 - 全局设置的 LACP 优先级值。可能范围为 1 至 65535。默认值为 1。

➢ 端口 - 显示要设定超时和优先级值的端口号。

➢ 端口优先级 - 显示端口的 LACP 优先级值，范围从“1-65535”。

➢ LACP 超时 - 管理 LACP 超时。

2. 设定 LACP 系统优先级后单击“提交”，参数将被保存并更新设备。

修改 LACP 参数：

1. 点击：网桥配置>接口>LACP 参数。打开接口 LACP 成员关系页面：

2. 点击✎，打开 LACP 参数设置页面：



图 7-6 LACP 参数设置页面

3. 设置 LACP 端口优先级与 LACP 超时字段。

4. 点击“提交”，LACP 设置被保存并更新设置。

7.3 配置VLAN

VLAN 是 LAN 的逻辑子组，它将用户站点和网络设备组合为单个单元，而不考虑它们连接的物理 LAN 网段。VLAN 使网络通信在子组内的传输更加有效。通过软件管理,VLAN 可减少执行网络更改、添加和移动所需的时间。

由于 VLAN 是基于软件，而不是通过物理属性进行定义的，因此 VLAN 可以拥有无限数量的端口，并且可以针对每个装置、设备、堆栈或任何其它逻辑连接组合进行创建。

VLAN 在第 2 层起作用。由于 VLAN 将通信隔离在 VLAN 内部，所以需要在第 3 层协议级别工作的路由器以允许通信在 VLAN 之间传输。第 3 层路由器使用 VLAN 标识网段和坐标。VLAN 是广播域和多点传送域。广播和多点传送通信仅在生成通信的 VLAN 中传输。

VLAN 标记提供了在 VLAN 组之间传输 VLAN 信息的方法。VLAN 标记可以将一个 4 字节标记附加至数据包标头。VLAN 标记表示数据包所属的 VLAN。VLAN 标记由终端站点或网络设备附加至 VLAN。VLAN 标记还可以包含 VLAN 网络优先级信息。

组合 VLAN 和 GVRP 使网络管理员可以将网络节点定义到广播域中。

这个部分包含下列主题：

➢ 定义 VLAN 属性

- 定义 VLAN 成员组
- 定义 VLAN 接口
- GARP 配置
- 定义 GVRP

7.3.1 定义VLAN属性

该页面提供 VLAN 配置的信息和所有参数。

添加一个新的 VLAN：

1、点击：网桥配置>VLAN>成员>属性，打开单个 VLAN 属性页面：



图 7-7 单个 VLAN 属性页面

单个 VLAN 属性页面包含以下字段：

- VLAN ID：显示在下面的 VLAN 表中选择的 VLAN 的属性。
- 全部显示：显示 VLAN 表中定义的所有 VLAN 的属性。
- VLAN
  - ID：显示 VLAN ID。
  - 名称：显示用户定义的 VLAN 名称。
- 类型：显示 VLAN 类型。可能的值是：
  - 动态：表示 VLAN 是由 GARP 动态创建的。
  - 静态：表示 VLAN 是用户定义的。
  - 默认：表示 VLAN 是默认 VLAN。
- 认证：表示未认证的用户是否可以访问一个来宾 VLAN。可能的值是：
  - 已启用：允许未认证用户使用来宾 VLAN。

– 禁用：禁止未认证用户使用来宾 VLAN。

➢ 删除：删除 VLAN。可能的值是：

– 选中：删除选中的 VLAN。

– 不选中：维持当前 VLAN。

添加一个新的 VLAN：

1. 单击“创建”，打开添加 VLAN 页面：

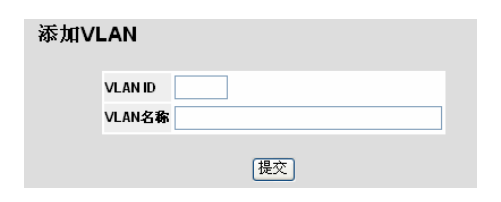


图 7-8 添加 VLAN 页面

2. 设置 VLAN ID 和 VLAN 名称。

3. 点击“提交”。新的 VLAN 被保存，并更新设备。

设置 VLAN 属性：

1. 点击✎，打开认证 VLAN 设置页面：



图 7-9 认证 VLAN 设置页面

2. 更改 VLAN 名称和禁用认证字段。

3. 点击“提交”，VLAN 属性被保存。

4. 在单个 VLAN 属性页面，点击“提交”，VLAN 信息被保存并更新设备。

7.3.2 定义VLAN成员组

VLAN 成员关系页面包含一张映射端口 VLAN 参数的表，各端口通过端口控制设置项被分配到 VLAN 成员组。

定义 VLAN 成员组页面：

1. 点击：网桥配置>VLAN>成员>成员，打开 VLAN 成员关系页面：

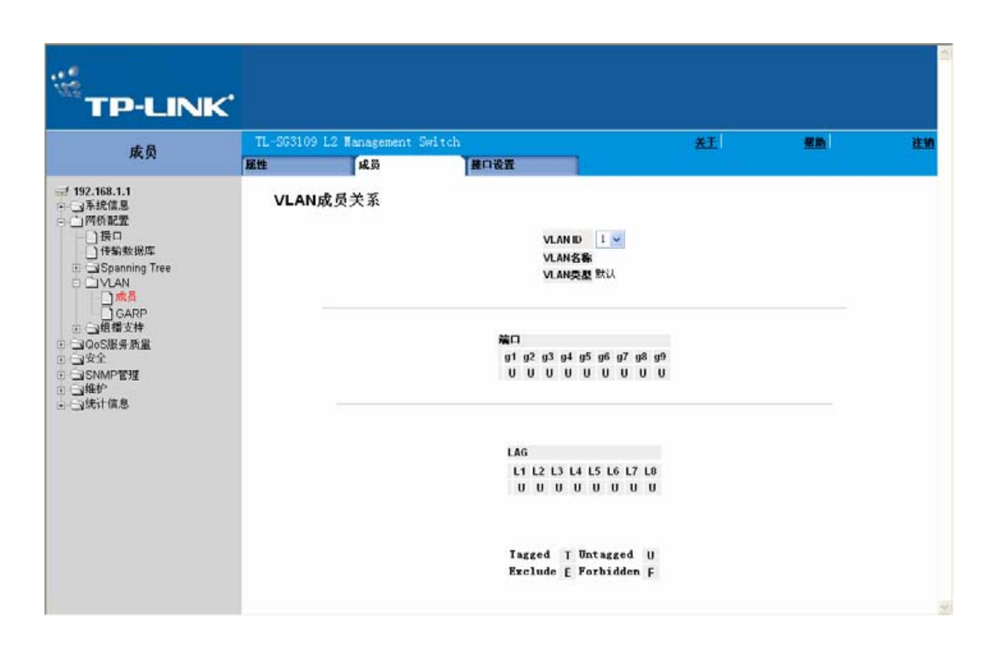


图 7-10 VLAN 成员关系页面

VLAN 成员关系页面包含以下字段：

- VLAN ID：显示用户定义的 VLAN ID。
- VLAN 名称：显示 VLAN 名称。
- VLAN 类型：显示 VLAN 类型。可能的值是：
  - 动态：表示 VLAN 是通过 GARP 动态创建的。
  - 静态：表示 VLAN 是由用户定义。
  - 默认：表示 VLAN 是默认的 VLAN。
- 端口：表示端口成员关系。
- LAG：表示 LAG 成员关系。
- U：表示接口是一个无标记 VLAN 的成员。被接口发送的数据包是无标记的。
- T：表示接口是一个带标记的 VLAN 的成员。接口发送的所有数据包都是有标记的。数据包包含 VLAN 信息。
- I：VLAN 中包含该端口。
- E：从 VLAN 排除接口。但是，接口可以通过 GARP 来加入 VLAN。
- F：拒绝接口的 VLAN 成员关系，即使 GARP 显示该端口已加入 VLAN。

定义 VLAN 接口设置

VLAN 接口设置页面提供了用于管理属于 VLAN 的端口。端口默认 VLAN ID 可在 VLAN 端口设置页面中进行配置。所有到达设备的未标记数据包均通过端口 PVID 进行标记。

7.3.3 定义VLAN接口

1. 点击：网桥配置>VLAN>成员>接口设置，打开接口设置页面：



图 7-11 接口设置页面

接口设置页面包含以下字段：

- 接口：显示包含在 VLAN 中的端口的编号。
- 接口 VLAN 模式：显示端口模式。可能的值是：
  - 常规：表示端口属于 VLAN，并且每个 VLAN 都是用户以加标记或去标记定义的（全 IEEE802.11q 模式）。
  - 访问：表示端口仅属于一个无标记的 VLAN。当端口是访问模式时，不可以指定在该端口上接收到的数据包的类型。不能在访问端口上启用或禁用接收过滤。
  - 主干：表示端口属于除一个端口可以去标记外所有端口都是加标记的 VLAN。
  - 动态：基于连接到端口的主机 MAC 地址来分配端口到一个 VLAN。
- PVID：分配一个 VLAN ID 给一个未标记的数据包。可能的值是 1-4094。按照标准和工业实际，4095 号 VLAN 被定义成丢弃 VLAN。分类到丢弃 VLAN 的数据包都将被丢弃掉。
- 帧类型：指定在端口上接受数据包的类型。可能的值是：
  - 仅接收 Tag：在端口上只接受收标记过的数据包。
  - 全部接受：在端口上接受标记过和未标记的数据包。
- 接收过滤：表示是否在端口上启用接收过滤。可能的值是：
  - 启用：在设备上启用接收过滤。接收过滤丢弃发送到指定端口不是 VLAN 的成员的数据包。

– 禁用：在设备上禁用接收过滤。

➢ 保留 VLAN：表示如果没有被系统使用则保留用户选择的 VLAN。

修改 VLAN 接口或 LAG 设置：

1. 点击✎，打开 VLAN 接口设置页面。



图 7-12 VLAN 接口设置页面

2. 修改端口接口，端口 VLAN 模式，PVID，帧类型，接收过滤，当前保留 VLAN，保留 VLAN 用于内部使用。

3. 点击“提交”，VLAN 或 LAG 接口配置完成并更新设备。

7.3.4 GARP配置

通用属性注册协议(GARP)是一个通用协议，用于注册所有网络连接信息或成员关系类型信息。GARP 定义了一组关于给定网络属性的设备，例如 VLAN 或组播地址。

配置 GARP 时，请确保满足以下要求：

➢ 离开时间必须大于或等于加入时间的三倍。

➢ 全部离开时间必须大于离开时间。

➢ 在第 2 层连接的所有设备上设置同一 GARP 计时器值。如果在第 2 层连接的设备上设置不同的 GARP 计时器，GARP 应用程序将不能成功运行。

定义 GARP：

1. 点击：网桥配置>VLAN>GARP>GARP 参数，打开 GARP 配置页面：



图 7-13 GARP 配置页面

GARP 配置页面包含以下字段：

- 从条目号：表示从选择的条目复制 GARP 参数。
- 复制到条目号：表示把 GARP 参数复制到选择的条目。
- 接口：显示启用了 GARP 的端口或 LAG。
- 加入计时器：以百分之一秒（厘秒）表示 PDU 传输的时间数。默认值是 20 厘秒。
- 离开计时器：以百分之一秒（厘秒）表示设备在离开其 GARP 状态前等待的时间数。离开时间是发送或解手全部离开消息激活，由受到加入消息取消。离开时间必须大于或等于 3 倍加入时间。默认值是 60 厘秒。
- 全部离开计时器：以百分之一秒（厘秒）表示在离开 GARP 状态前全部设备等待的时间数。全部离开时间必须大于离开时间。默认值是 1000 厘秒。

2. 在“从条目号”字段，输入接口号，在“复制到条目号”字段，输入需要的接口号。

3. 点击“提交”，修改 GARP 参数，并更新设备。

修改 GARP 设置：

1. 点击旁边的 修改，打开 GARP 参数设置页面：



图 7-14 GARP 参数设置页面

2. 修改计时器参数。

3. 点击“提交”，修改 GARP 参数，并更新设备。

7.3.5 定义GVRP

GARP VLAN 注册协议(GVRP)专用于在可识别 VLAN 的网桥之间自动分配 VLAN 成员关系信息。GVRP 使可识别 VLAN 的网桥能够自动学习 VLAN 到网桥端口的映射，而无需逐个配置每个网桥并注册 VLAN 成员关系。

定义 GVRP

1. 点击：网桥配置>VLAN> GARP>GVRP 参数，打开 GVRP 状态页面：



图 7-15 GVRP 状态页面

GVRP 状态页面包含以下字段：

- 从条目号复制：表示从选择的条目复制 GARP 参数。
- 到条目号：表示把 GARP 参数复制到选择的条目。
- 接口：显示启用了 GVRP 的接口。可能的值是：
  - 端口：显示启用了 GVRP 的端口的编号。
  - LAG：显示启用了 GVRP 的 LAG 的编号。
- GVRP 状态：表示是否在端口上启用 GVRP。可能的值是：
  - 已启用：在选择的端口上启用 GVRP。
  - 已禁用：在选择的端口上禁用 GVRP。

- 动态 VLAN 创建：表示是否在接口上动态创建 VLAN。可能的值是：
  - 已启用：启用在接口上动态创建 VLAN。
  - 已禁用：禁用在设备上动态创建 VLAN。
- GVRP 注册：表示是否在设备上启用通过 GVRP 注册 VLAN。可能的值是：
  - 已启用：在设备上启用 GVRP 注册。
  - 已禁用：在设备上禁用 GVRP 注册。

2. 选取 GVRP 全局状态并点击“提交”，保存全局 GVRP 参数。

修改全局 GVRP 或 LAG 参数：

1. 点击 GVRP 或 LAG 全局接口设置旁边的✎，打开 GVRP 参数设置页面：



图 7-16 GVRP 参数设置页面

2. 启用或禁用 GVRP 状态，动态 VLAN 创建和 GVRP 注册。
3. 点击“提交”，修改全局 GVRP 或 LAG 参数，并更新设备。

第8章　　定义传输数据库

目的地址存储在静态地址或动态地址数据库中的数据包被立即转发至端口。动态地址表可以按接口、VLAN 和 MAC 地址进行分类。当数据包从源到达设备时，MAC 地址将被动态学习。静态地址是手动配置的。

通过从帧的源地址学习端口，可以将地址与端口相关联。但是定址与任一端口均不相关的目的地MAC 地址的帧将被多路发送至相关 VLAN 的所有端口。为防止桥接表溢出，在特定时间段内未进行任何通信的动态 MAC 地址将被删除。

这部分包括定义双方静态和动态转发地址，并包含下列主题：

- 静态地址配置
- 动态传输地址配置

8.1 静态地址配置

传输数据库的静态地址页面包含定义设备的老化时间参数。防止静态 MAC 地址在设备重新复位后被删除，确保 MAC 地址绑定到端口。

定义传输数据库的静态地址：

1. 点击：网桥配置>传输数据库>静态地址，打开静态地址页面：



图 8-1 静态地址页面

静态地址页面包含以下字段：

- VLAN ID：显示条目涉及的 VLAN ID 号。
- MAC 地址：显示条目涉及的 MAC 地址。
- 接口：显示条目涉及的接口。
    - 端口：指定传输数据库参数涉及的端口号。
    - LAG：指定传输数据库参数涉及的 LAG 号。

– 状态：显示条目是如何创建的。可能的值是：

– 安全：MAC 地址为锁定端口定义。

– 永久：MAC 地址是永久地址。

– 复位时删除：当设备复位时删除 MAC 地址。

– 超时时删除：当超时发生时删除 MAC 地址。

➢ 删除：删除条目。可能的值是：

– 选中：删除选中的条目。

– 不选中：维持当前静态传输数据库。

2. 点击“创建”，打开添加传输数据库页面：



图 8-2 添加传输数据库页面

3. 定义接口，MAC 地址，VLAN ID 和 VLAN 名称，状态字段。

4. 点击“提交”，更改传输数据库信息，并更新设备。

8.2 动态传输地址配置

动态地址页面包含用于查询动态地址表中的信息,包括接口类型、MAC 地址、VLAN 和表存储的信息。页面还包含有关动态 MAC 地址被删除前存在时间的信息，并包括用于查询和查看动态地址列表的参数。动态地址表包含将数据包直接传输至那些端口所依据的地址参数。动态地址表可以按接口、VLAN 或 MAC 地址排序。

定义动态传输地址：

1. 点击：网桥配置>传输数据库>动态地址，打开动态地址页面：



图 8-3 动态地址页面

动态地址页面包含以下字段：

- 老化时间（秒）：以秒指定如果没有在源端口检测到流量时，MAC 地址在超时前保存在动态 MAC 地址表中的时间数，默认值是 300 秒。
- 清除表格：清除当前地址表。

查询于部分包含以下字段：

- 接口：指定查询表的接口（端口或 LAG）。
- MAC 地址：指定查询表的 MAC 地址。
- VLAN ID：指定查询表的 VLAN ID。
- 地址表排列方式：指定地址表以何种方式排列。地址表可以地址，VLAN 或接口排列。

当前地址表显示动态地址定义的：VLAN ID，MAC 和接口等部分参数。

2. 点击“上一页”、“下一页”浏览地址表。

查询动态地址表：

1. 点击：网桥配置>传输数据库>动态地址，打开动态地址页面。
2. 选择接口，MAC 地址，VLAN ID。
3. 选择一个地址表排列方式关键字。
4. 点击“查询”，查询动态 MAC 地址表并在当前地址表显示结果。

第9章　　配置生成树协议

生成树协议(STP)提供了树拓扑，用于任意网桥排列。STP 同时在网络中的终端站点之间提供一条路径消除了环路。

主机之间存在备用路由时，将形成环路。扩展网络中的环路可能会造成网桥无限制地传输通信，从而导致通信量增加以及网络效率降低。

设备支持以下生成树版本：

- 经典 STP：在终端站点之间提供单一路径，以避免并消除环路。有关配置经典 STP 的详细信息，请参阅经典 STP 配置。
- 快速 STP：检测并使用提供快速生成树聚合的网络拓扑，且不会创建传输环路。有关配置快速 STP 的详细信息，请参阅快速 STP 配置。
- 多重 STP：提供多种负载均衡，例如，端口 A 在一个生成树中被阻止，此端口能在另一个生成树中处于转发状态。有关配置多重 STP 的详细信息，请参阅多重 STP 配置。

这个部分包含下列主题：

- 经典 STP 配置
- 快速 STP 配置
- 多重 STP 配置

9.1 经典STP配置

这个部分描述下列主题：

- 定义 STP 属性
- STP 接口设置

9.1.1 定义STP属性

STP 常规页面包含在设备上启用 STP 的参数。

定义 STP 属性：

1. 点击：网桥配置>Spanning Tree>STP>属性，打开 STP 常规页面：



图 9-1 STP 常规页面

STP 常规页面包含以下字段：

- 生成树（STP）状态：显示是否在设备上启用 STP。可能的值是：
  - 启用：在设备上启用 STP。
  - 禁用：在设备上禁用 STP。
- STP 运行模式：在启用了 STP 的设备上指定 STP 模式。可能的值是：
  - 标准生成树（STP）：在设备上启用标准生成树。这是默认值。
  - 快速生成树（RSTP）：在设备上启用快速生成树。
  - 多重生成树（MSTP）：在设备上启用多重生成树。
- BPDU 处理：决定当在端口或设备上禁用 STP 时如何管理 BPDU 数据包。

BPDU 用来传输生成树信息。可能的值是：

  - 过滤：当在端口上禁用生成树时过滤 BPDU 数据包。这是默认值。
  - 多路发送：当在端口上禁用生成树时多路发送 BPDU 数据包。
- 路径开销默认值：指定给 STP 端口分配默认路径开销的方式。可能的值是：
  - 短：为端口指定从 1 到 65535 的路径开销。这是默认值。
  - 长：为端口指定从 1 到 200，000，000 的路径开销。为端口分配的默认路径开销将根据选择的方式（联络时间，最长存在时间，发送延迟）而改变。

网桥设置部分包含以下字段：

- 优先级：指定网桥优先级值。当交换机或网桥运行 STP 时，每个设备都将被赋予一个优先级。在交换 BPDU 后，拥有低优先级值的设备成为根网桥。默认值是 32768。端口优先级值的增量是 4096。

- 联络时间：指定设备的联络时间。联络时间是根网桥等待配置消息的以秒计的时间数。默认值是 2 秒。

- 最长存在时间：指定设备的最长存在时间。最长存在时间是网桥发送配置消息前等待的以秒计的时间数。默认最长存在时间是 20 秒。

- 传输延迟：指定设备的发送延迟时间。发送延迟时间是网桥在发送数据包前维持在监听和学习状态的以秒计的时间数。默认值是 15 秒。

指定根部分包含以下字段：

- 网桥 ID：显示网桥优先级和 MAC 地址。

- 根网桥 ID：显示根网桥优先级和 MAC 地址。

- 根端口：显示提供从本网桥到根网桥具有最低路径开销的端口号。当网桥不是根网桥时该项目很重要。默认值是 0。

- 根路径开销：从本网桥到根网桥的路径开销。

- 拓扑改变计数：指定 STP 状态已经改变的总次数。

- 上次拓扑改变：显示自网桥初始化或复位，以及上次发生拓扑改变以来的总时间。该时间以 D/H/M/S 格式显示，例如 2 天/5 小时/10 分/4 秒显示为 2D/5H/10M/4S。

2. 定义生成树状态和网桥设置字段。

3. 点击“提交”。添加新的 STP 定义并更新设置信息。

9.1.2 STP接口设置

使用 STP 接口设置页网络管理员可以在指定的接口上进行 STP 设置。全局 LAG 部分显示链路汇聚组的 STP 信息。

分配 STP 设置到一个接口：

1. 点击：网桥配置>Spanning Tree>STP>接口设置，打开接口配置页面：

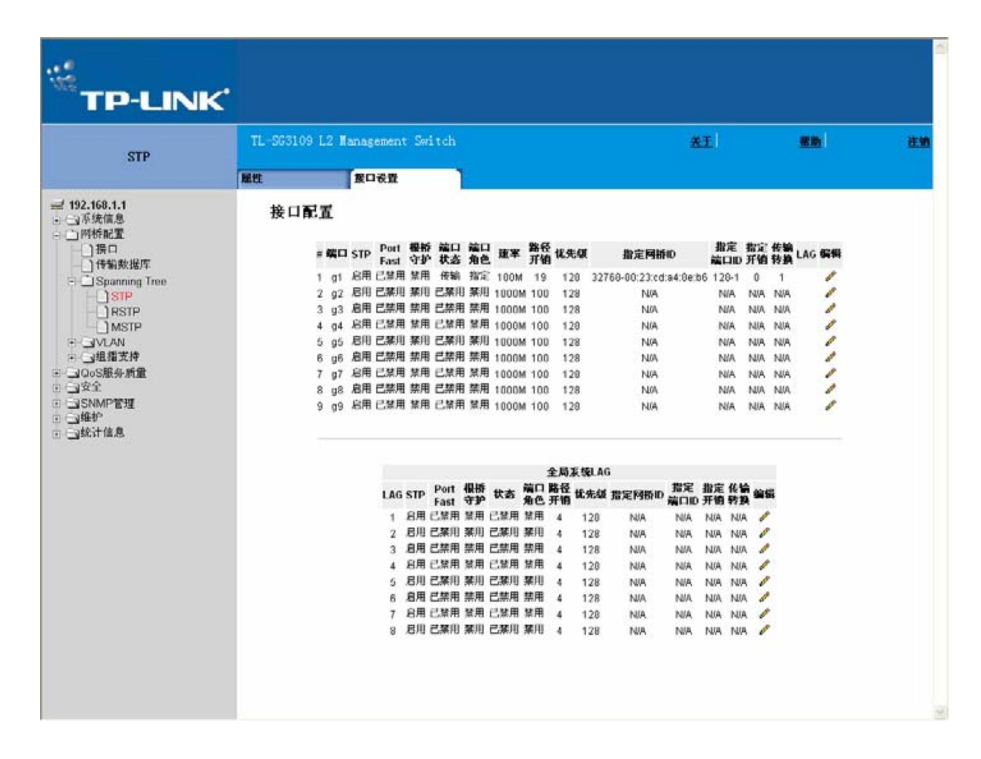


图 9-2 接口配置页面

接口配置页面包含以下字段：

- 端口：显示端口信息。
- STP：显示是否在端口上启用 STP。可能的值是：
  - 启用：在端口上启用 STP。
  - 禁用：在端口上禁用 STP。
- Port Fast：显示在端口上是否启用了 Port Fast。如果为一个端口启用了 Port Fast,当该端口连接的时候就自动处于发送状态。Port Fast 优化 STP 协议的收敛。在一个大的网络中，STP 收敛可能会用时 30-60 秒。
- 根桥守护：防止处于网络边缘的设备被指派成生成树的根。
- 端口状态：显示端口的当前 STP 状态。如果启用，端口状态就会决定在数据流上采取什么样的发送行为。可能的端口状态有：
  - 已禁用：显示端口当前是禁用 STP 的。当端口学习到 MAC 地址时就发送数据流。
  - 传输：显示端口当前被锁定并且不能发送数据流或学习 MAC 地址。当启用了标准 STP 时，就显示锁定状态。
- 速率：显示端口的工作速率。
- 路径开销：显示端口分担的到根的路径开销。当一条路径重新选路后，可以将路径开销值调高一点或低一点来发送数据流。
- 优先级：显示端口的优先级值。当网桥有两个端口连接到一环路时，优先级值会影响端口选择。优先级值范围是从 0-240。优先级值的增量是 16。

➢ 指定网桥 ID：显示指定网桥的网桥优先级和 MAC 地址。

➢ 指定端口 ID：显示选择的端口优先级和接口。

➢ 指定开销：显示端口在 STP 拓扑中传输的开销。如果 STP 检测到环路，低开销的端口被锁定的可能要低一些。

➢ 传输转换：显示端口从发送状态变为锁定状态后的时间。

➢ LAG：显示端口从属的 LAG。

修改 STP 设置：

2. 点击，打开接口设置页面：



图 9-3 接口设置页面

3. 在 STP 下拉列表中选择启用 STP 功能。

4. 设定所有字段。

5. 点击“提交”，修改选定的接口设置，并更新设备信息。

9.2 快速STP配置

虽然经典生成树可以防止普通网络拓扑中出现第 2 层传输环路，但聚合需要花费 30 至 60 秒。这段时间将延迟对可能存在的环路的检测，并传播状态更改。快速生成树协议(RSTP)可以检测并使用允许生成树快速聚合的网络拓扑，且不会创建传输环路。全局系统 LAG 信息显示与端口相同的字段信息，但它是 LAG 快速生成树信息。

定义快速生成树：

1. 点击：网桥配置>Spanning Tree>RSTP> RSTP，打开 RSTP 页面：

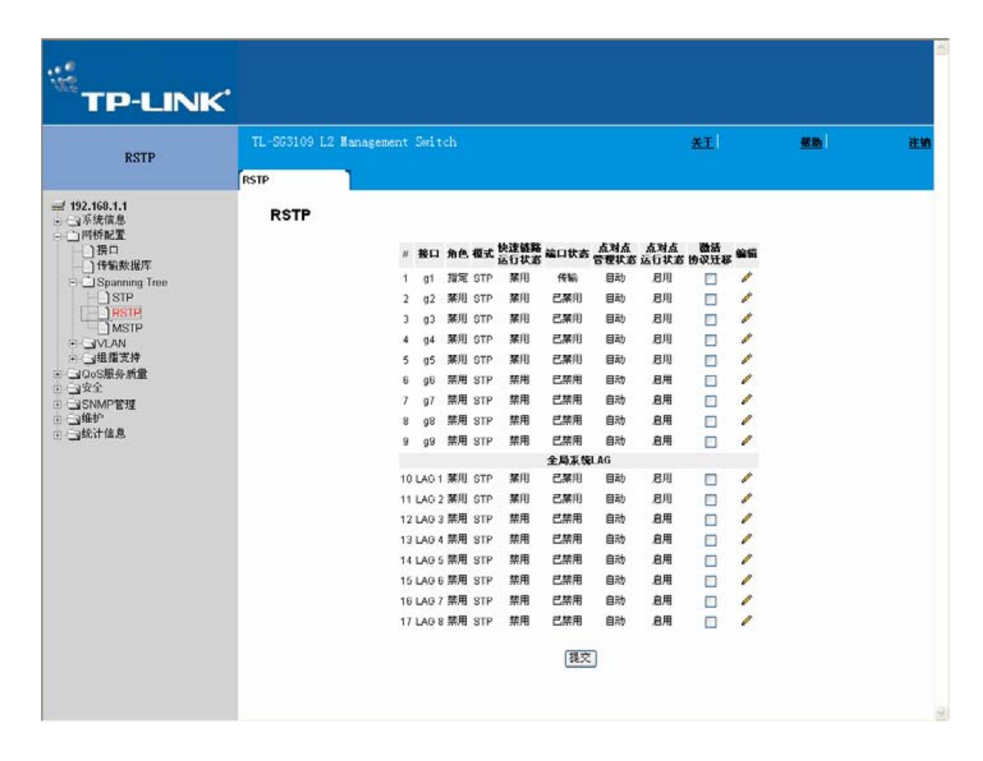


图 9-4 RSTP 页面

RSTP 页面包含以下字段：

➢ 接口：显示启用了快速 STP 的端口或 LAG。

➢ 端口状态：显示启用了 RSTP 的端口的 RSTP 状态。可能的值是：

– 已禁用：显示端口当前禁用了 RSTP。

– 传输：显示端口当前使用 RSTP 来连接和发送流量。

➢ 角色：显示由 STP 算法分配给 STP 路径的端口角色。可能的值是：

– 根：提供发送数据包到根交换机的最低开销路径。

– 指定：显示连接指定交换机到 LAN 的端口或 LAG。

– 替代：提供从根接口到根交换机的替代路径。

– 备份：给指定端口到生成树叶接点的路径提供一个备份路径。只有当两个端口由点对点连接成一个环路或当 LAN 有两个或更多的链路连接到同一共享网段时才发生备份端口事件。

– 禁用：显示端口不参与生成树。

➢ 模式：显示当前 STP 模式。在 STP 属性页面上选择 STP 模式。可能的值是：

– STP：表示在设备上启用标准 STP。

– RSTP：表示在设备上启用 RSTP。

– MSTP：表示在设备上启用 MSTP。

➢ 快速链路运行状态：显示端口或 LAG 是否启用或禁用快速链路。如果启用端口的快速链路，端口将自动进入发送状态。

➢ 点对点管理状态：显示是否建立了一个点对点连接，或设备是否允许建立点对点连接。可能的值是：

– 启用：设备允许建立点对点连接，或是被配置成自动建立点对点连接。为在点对点链路上通信，源 PPP 首先发送链路控制协议（LCP）数据包来配置和测试数据链路。当建立起连接和可选设备按照 LCP 要求的那样协商好之后，源 PPP 发送网络控制协议（NCP）数据包来选择和配置一个或多个网络层协议。当每个选择的网络层协议都已配置好后，来自每个网络层的数据包就可以在链路上发送。链路为通信维持配置直到显式的 LCP 或 NCP 数据包关闭连接，或直到某些外部事件发生。这是实际的交换机端口连接类型。它可以不同于管理状态。

– 禁用：禁用点对点连接。

– 自动：自动启用点对点连接。

➢ 点对点运行状态：显示点对点运行状态。

➢ 激活协议迁移

2. 点击✎，打开快速生成树（RSTP）设置页面：



图 9-5 快速生成树（RSTP）设置页面

快速生成树（RSTP）设置页面包含以下字段和列在 RSTP 页面里的设置项。

➢ 激活协议迁移测试：表示是否发送链路控制协议(LCP)数据包配置和检测数据链路。可能的选项值是：

– 选中：允许发送协议。

– 不选中：不允许发送协议。

3. 在 RSTP 设置页中，需要修改以下字段：点对点管理状态，点对点运行状态。

4. 选中激活协议迁移测试复选框。

5. 点击“提交”。

6. 在 RSTP 页面点击“提交”，保存 RSTP 参数，并更新设备。

9.3 多重STP配置

多重生成树提供了不同的负载平衡方案。例如，一个 STP 实例中的端口 A 处于阻塞状态时，该端口在另一个 STP 实例中处于转发状态。

这个部分包含下列主题：

- 定义 MSTP 属性
- 配置 MSTP 实例
- 配置 MSTP VLAN 实例
- 配置 MSTP 接口

9.3.1 定义MSTP属性

MSTP 常规页面包含了定义全局 MSTP 的信息，包括区域名，MSTP 修正和最大路程段。

定义 MSTP：

1. 点击：网桥配置>Spanning Tree>MSTP>属性，打开 MSTP 常规页面：



图 9-6 MSTP 常规页面

MSTP 常规页面包含以下字段：

- 区域名称：表示用户定义的 STP 区域名称。
- 版本：定义标识当前 MST 配置版本的无符号 16 位数字。版本号是 MSTP 配置所需的一部分。可能的字段范围是 0 至 65535。
- 最大路程段：定义在丢弃 BPDU 以前特定区域中所出现的路程段总数。丢弃 BPDU 后，端口信息将过期。可能的字段范围为 1 至 40。字段默认值为 20 个路程段。
- 主 IST：确定生成树的主 IST 实例。主 IST 为指定实例的根。

2. 设定区域名称，版本和最大路程段字段。

3. 点击“提交”，更新设备信息。

9.3.2 配置MSTP实例

MSTP 操作将 VLAN 映射至 STP 实例中。分配至不同 VLAN 的数据包将在多重生 成树区域（MST 区域）内部沿不同路径发送。区域为一个或多个可用于传输帧的 多重生成树网桥。配置 MSTP 时设备所属的 MSTP 区域是已定义的。配置包含设 置所属的名称，版本和区域。

使用 MSTP 接口设置页面网络管理员可以定义 MSTP 接口设置。

为 MSTP 定义接口设置：

1. 点击：网桥配置>Spanning Tree>MSTP>实例设置，打开修改 MSTP 实例页 面：



图 9-7 修改 MSTP 实例页面

修改 MSTP 实例页面包含以下字段：

- 实例 ID：指定分配接口的 VLAN 组。
- 包括的 VLAN：映射选择的 VLAN 到选择的实例。每个 VLAN 属于一个实例。
- 网桥优先级：指定选择的生成树实例设备优先级。该值范围是 0-61440。
- 指定根网桥 ID：显示到实例 ID 的具有最低路径开销的网桥 ID。
- 根端口：显示选择的实例的根端口。
- 根路径开销：显示选择的实例的路径开销。
- 网桥 ID：显示选择的实例的网桥 ID。
- 剩余路程段：显示到下一目的地的剩余路程段数。

2. 设定字段。

3. 点击“提交”，保存 MSTP 设置并更新设备。

9.3.3 配置MSTP VLAN实例

网络管理员能为 VLAN 实例分配 MSTP。

为 VLAN 接口定义 MSTP：

1. 点击：网桥配置>Spanning Tree>MSTP>实例设置>VLAN 实例配置，打开 VLAN 实例配置页面：

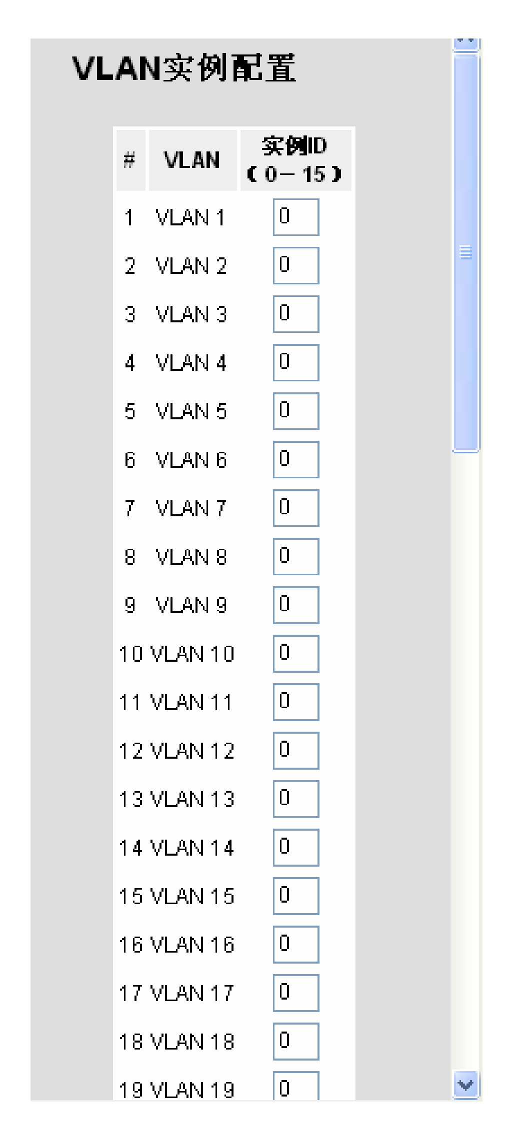


图 9-8 VLAN 实例配置页面

VLAN 实例配置页面包含以下字段：

- VLAN：映射选中的 VLAN 到选定的实例。一个 VLAN 属于一个实例。
- 实例 ID（0-15）：指定接口被分配的 VLAN 组。

添加一个新的 VLAN 实例：

1. 选取一个 VLAN 并输入实例 ID。

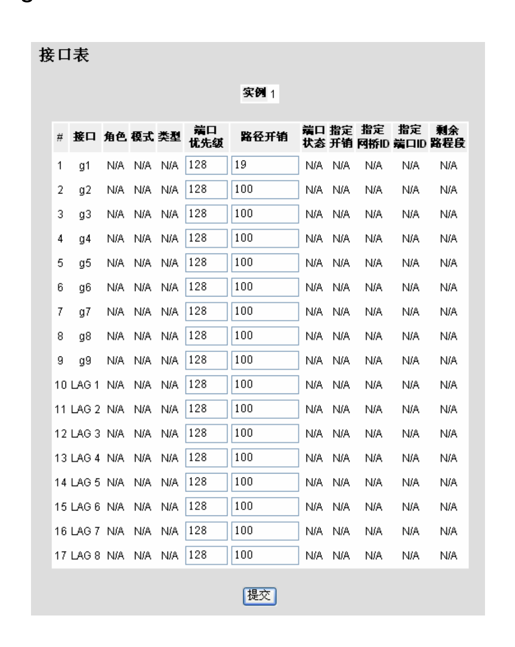
2. 点击“提交”，更新设置信息。

9.3.4 配置MSTP接口

网络管理员能在 MSTP 接口设置页面指定 MSTP 接口设置。

为 MSTP 定义接口：

1. 点击：网桥配置>Spanning Tree>MSTP>接口设置>接口表，打开接口表页面：



接口表

实例 1

#	接口	角色	模式	类型	端口优先级	路径开销	端口状态	指定开销	指定网桥ID	指定端口ID	剩余路程段
1	g1	N/A	N/A	N/A	128	19	N/A	N/A	N/A	N/A	N/A
2	g2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
3	g3	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
4	g4	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
5	g5	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
6	g6	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
7	g7	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
8	g8	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
9	g9	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
10	LAG 1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
11	LAG 2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
12	LAG 3	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
13	LAG 4	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
14	LAG 5	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
15	LAG 6	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
16	LAG 7	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
17	LAG 8	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A

提交

图 9-9 接口表页面

接口表页面包含以下字段：

- 实例：列出设备上配置的 MSTP 实例。可能的字段范围是 0 至 15。
- 接口：显示 MSTP 接口设置。可能的字段值是：
  - 端口：显示的是为 MSTP 指定的是端口。
  - LAG：显示的是为 MSTP 指定的 LAG。
- 角色：表示由 STP 算法分配的以便提供 STP 路径的端口角色。可能的字段值包括：
  - 根：提供最低成本路径以将数据包传输给根设备。
  - 指定：表示指定的设备连接至 LAN 所通过的端口或 LAG。
  - 备用：通过根接口向根设备提供备用路径。
  - 备份：提供去往生成树树叶的指定的端口路径的备份路径。仅当两个端口通过点对点链路连接在一个环路中时，才会出现备份端口。当 LAN 有两个或多个连接到一个共享网段的连接时，也会出现备份端口。
  - 禁用：表示端口未加入生成树。

- 模式：表示在设备上启用的生成树模式。可能的字段值包括：
  - 经典 STP：表示在设备上启用经典 STP。这是默认值。
  - 快速 STP：表示在设备上启用快速 STP。
  - 多重 STP：表示在设备上启用多重 STP。
- 类型：表示端口是边界端口还是主端口，可能的值是：
  - 边界端口：表示端口是一个边界端口，边界端口将 MST 网桥连接至远端区域中的 LAN。如果端口为边界端口，它还可以表示链路另一端的设备是以 RSTP 模式还是以 STP 模式工作。
  - 主端口：表示端口是一个主端口，主端口提供从 MSTP 区域到远端 CIST 根的连接。
- 端口优先级：定义指定实例的端口优先级。默认值为 128。
- 路径开销：表示端口在生成树实例中所占的比例。范围应始终为 1 至 200,000,000。
- 端口状态：表示指定实例的端口是否启用，可能的字段值有：
  - 启用：启用指定实例的端口。
  - 禁用：禁用指定实例的端口。
- 指定开销：表示根据“Spanning Tree Global Settings”（生成树全局设置）页面上选择的方法分配默认路径成本。
- 指定网桥 ID：显示将链路或共享 LAN 连接至根的网桥 ID 号。
- 指定端口 ID：显示将链路或共享 LAN 连接至根的指定网桥上的端口 ID 号。
- 剩余路程段：表示距下一个目的地的剩余路程段数。

2. 选择实例。
3. 修改端口优先级和路径开销。
4. 点击“提交”，更新设备信息。

为 MSTP 添加新的接口设置：

1. 设定接口属性字段，如下图：



图 9-10 修改接口页面

2. 点击“提交”，添加接口设置到 MSTP 接口设置页面列表，并更新设备信息。

第10章　配置组播转发

组播转发使数据包可以从任一个特定的组播组传输至一个源，或者从一个不特定的源到一个组播组。

这个部分包含下列主题：

- 启用 IGMP 侦听
- 定义组播组
- 定义全部组播发送属性

10.1 启用IGMP侦听

全局启用 IGMP 监测时，所有 IGMP 数据包将传输至 CPU。CPU 将分析传入的数据包，并确定：

- 哪些端口要加入哪些组播组。
- 哪些端口具有生成 IGMP 查询的多点传送路由器。
- 哪些路由协议传输数据包和组播通信。

请求加入特定组播组的端口将发出 IGMP 报告，指明该组播组正在接受成员。这将导致创建组播过滤数据库。

启用 IGMP 侦听：

1. 点击：网桥配置>组播支持>IGMP 侦听，打开 IGMP 侦听页面：



图 10-1 IGMP 侦听页面

IGMP 侦听页面包含以下字段：

- 启用 IGMP 侦听：表明在设备上是否启用了 IGMP 侦听。仅当网桥组播过滤启用时 IGMP 侦听才能被启用。可能的值是：
  - 选中：在设备上启用 IGMP 侦听

– 不选中：在设备上禁用 IGMP 侦听。

➢ VLAN ID：指定 VLAN ID。

➢ IGMP 侦听状态：表示是否在 VLAN 上启用 IGMP 侦听。可能的值是：

– 已启用：在 VLAN 上启用 IGMP 侦听。

– 已禁用：在 VLAN 上禁用 IGMP 侦听。

➢ 自动学习：表示是否在设备上启用自动学习。如果启用了自动学习，设备将在发现其他组播组时自动学习。在以太网设备上启用或禁止自动学习。可能的值是：

– 已启用：启用自动学习。

– 已禁用：禁止自动学习。

➢ 主机超时：表示主机在超时前等待接收信息的时间数。默认值是 260 秒。

➢ 多点传送路由器超时：表示多点传送路由器在超时前等待接收信息的时间数。默认值是 300 秒。

➢ 离开超时：表示在超时前，主机在请求离开 IGMP 组后没有从别的主机收到加入消息后等待的时间数。如果发生了离开超时，交换机通告组播设备停止发送流量。离开超时值可以是用户自定义的或是一个立即离开值。默认值是 10 秒。

2. 选中启用 IGMP 侦听复选框。

3. 点击“提交”，在设备上启用 IGMP 侦听。

修改 IGMP 侦听：

1. 点击✎，打开组播全局参数设置页面：



图 10-2 组播全局参数设置页面

2. 修改 VLAN ID，IGMP 状态启用，自动学习，主机超时，多点传送路由器超时，离开超时等字段。

3. 点击“提交”，修改 IGMP 全局属性，并更新设备。

10.2 定义组播组

组播组表页面用端口表和 LAG 表的方式显示加入到组播服务组的端口和 LAG。端口和 LAG 表同时反映端口或 LAG 加入组播组的方式。端口可以加入已存在的组或新的组播服务组。组播组表页面允许创建新的组播服务组。组播组表页面也可以分配端口到指定的组播服务地址组。

定义组播组：

1. 点击：网桥配置>组播支持>网桥组播>组播组，打开组播组表页面：

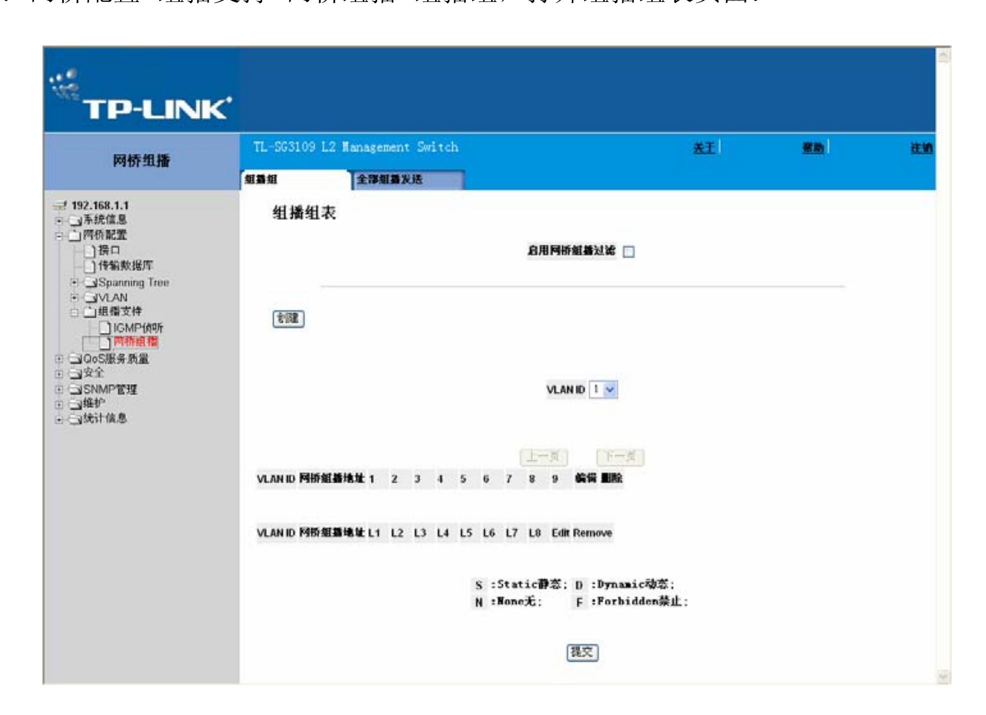


图 10-3 组播组表页面

组播组表页面包含以下字段：

- 启用网桥组播过滤：表示在设备上启用网桥组播过滤。可能的值是：
  - 选中：在设备上起用组播过滤
  - 不选中：在设备上禁止组播过滤。如果禁止了组播过滤，组播帧将被多点发送到相关 VLAN 的所有端口。禁止是默认值。
- VLAN ID：标志 VLAN 并且包含关于组播组地址的信息。
- 网桥组播地址：标志组播组的 MAC 地址/IP 地址。
- 端口：显示可以加入到组播服务的端口。
- LAG：显示可以加入到组播服务的 LAG。

以下表格包含 IGMP 端口和 LAG 成员管理设置：

端口控制	定义
D	端口/LAG 已动态加入当前行中的组播组。
S	将端口作为静态行中的静态成员连接至组播组。 端口/LAG 已静态加入当前行中的组播组。
F	禁止未包含在组播组的端口，即使是 IGMP 侦听指定的端口加入一个组播组。
空白	端口未连接至组播组。

表 10-1 IGMP 端口/LAG 成员表控制设置

2. 点击“创建”，打开添加组播组页面：

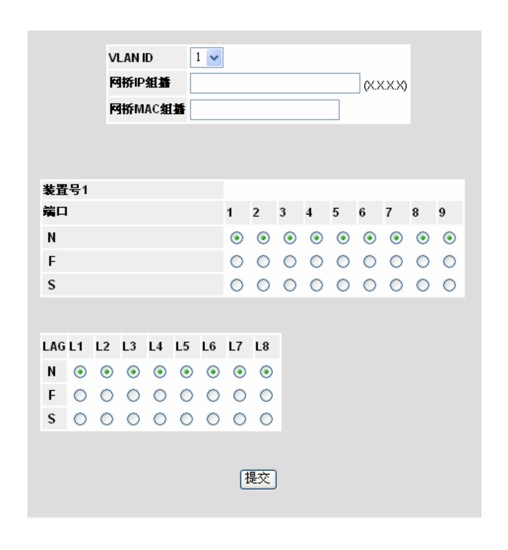


图 10-4 添加组播组页面

3. 设定 VLAN ID，网桥 IP 组播，网桥 MAC 组播等字段。

4. 点击“提交”。

5. 在组播组表页面，选择端口加入到组播组。

6. 设定组播端口。

7. 点击“提交”，完成组播组表设定，并更新设备。

修改组播组设置：

1. 点击：网桥配置>组播支持>网桥组播>组播组，打开组播组表页面。单击，打开组播组设置页面：

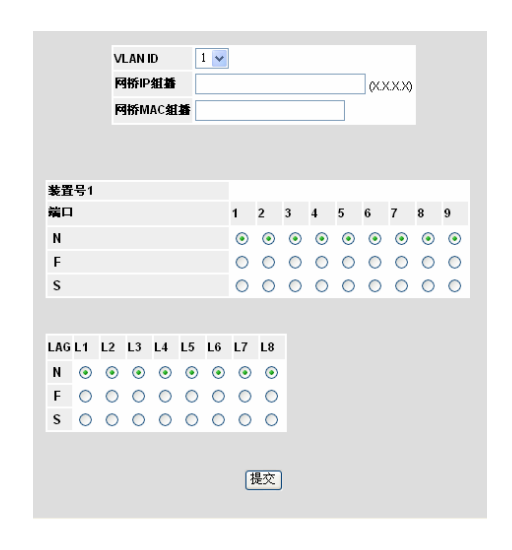


图 10-5 组播组设置页面

2. 选择 VLAN 的端口/LAG 并定义端口设置。

3. 点击“提交”，修改完成组播组设置并更新设备信息。

10.3 定义全部组播发送属性

全部组播发送页面包含加入端口或 LAG 到一个连接到邻接组播路由器或交换机的设备的字段。一旦启用 IGMP 侦听，组播数据包将被发送到相应的端口或 VLAN。除非定义了 LAG，否则只显示全部组播发送表。

设置全部组播发送属性：

1. 点击：网桥配置>组播支持>网桥组播>全部组播发送，打开全部组播发送页面：

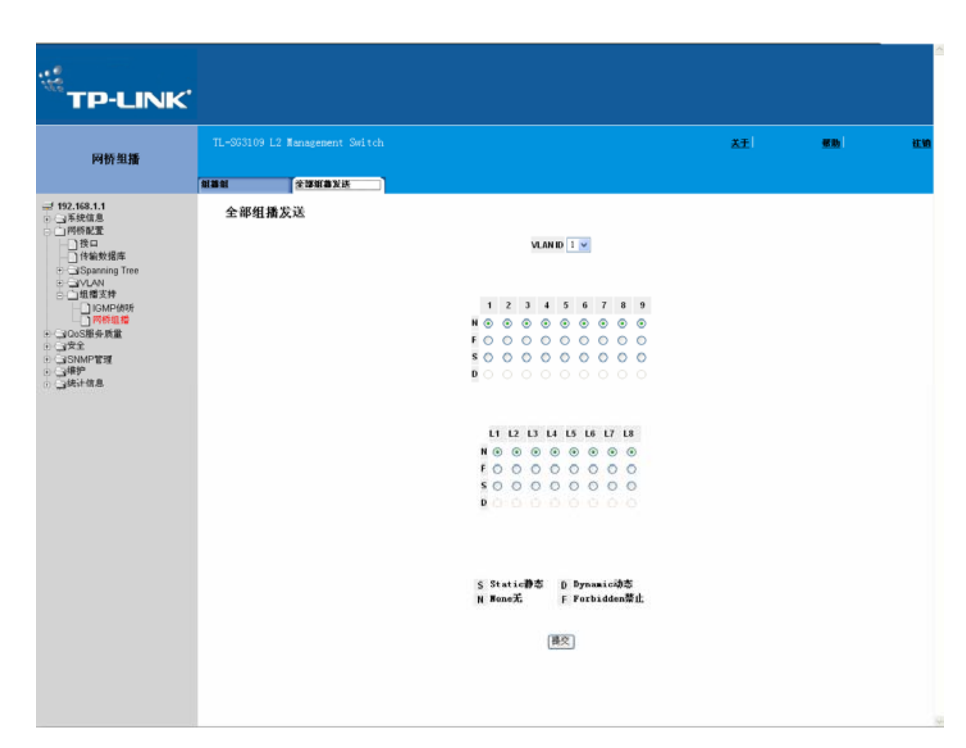


图 10-6 全部组播发送页面

全部组播发送页面包含以下字段：

- VLAN ID：列出显示组播参数的 VLAN。
- 端口/LAG：能被加入到一个组播设备的端口。

下面的表格概括了分配给端口的组播设置。

端口控制	定义
D	添加端口到组播路由器或交换机作动态端口。
S	添加端口到组播路由器或交换机作静态端口。
F	禁止。
N	端口不能添加到一个组播路由器或交换机。

表 10-2 网桥组播转发路由/端口控制设置表

2. 在 VLAN ID 下拉列表中选择一个 VLAN。
3. 设定 VLAN 端口。
4. 点击“提交”，设定选定 VLAN 的组播转发设置并更新设备。

第11章　配置SNMP管理

简单网络管理协议（SNMP）提供了一种管理网络设备的方法。这种设备支持下列 SNMP 版本：

- SNMP 版本 1
- SNMP 版本 2c
- SNMP 版本 3

这部分包含以下主题：

- SNMP 版本 1 和版本 2c
- SNMP 版本 3
- 定义 SNMP 安全性
- SNMP 报告设置

11.1 SNMP版本 1 和版本 2c

SNMP 代理维持一系列的管理网络设备的变量。这些变量是在管理信息库中被定义的。SNMP 代理定义了 MIB 的特殊格式，同时也定义了在网络外访问信息的格式。SNMP 代理的访问权由访问字符串控制。

11.2 SNMP版本 3

SNMP 版本 3 应用于访问控制和一种新的陷阱机制。另外，版本 3 定义了用户安全模型参数，包含以下：

- 授权：提供数据的完整性和数据的原始授权。
- 个人密钥：保护信息内容不外泄。CBC 用于加密。在 SNMP 信息中使用授权，或者授权和个人密钥两者都使用。然而，在没有授权的情况下，个人密钥是不起作用的。
- 合时性：防止信息延迟和信息冗余。SNMP 代理把进入的信息与时间信息比较。
- 密钥管理：定义密钥的生成，更新和使用。

设备支持基于对象标识的 SNMP 通告过滤。对象标识被系统用来管理设备。SNMP 版本 3 支持以下功能：

- 安全性
- 访问控制
- 陷阱

设备生成下列陷阱：

➢ 复制陷阱

11.3 定义SNMP安全性

这部分描述了 SNMP 安全性参数的配置，包括下列主题：

➢ 定义 SNMP 全局参数

➢ 定义 SNMP 视图

➢ 定义 SNMP 组

➢ 定义 SNMP 组成员

➢ 定义 SNMP 团体

11.3.1 定义SNMP全局参数

SNMP 安全性全局参数页面允许使用 SNMP 和授权通告。

定义 SNMP 安全性全局参数：

1. 点击：SNMP 管理>安全>全局参数，打开引擎 ID 页面：



图 11-1 引擎 ID 页面

引擎 ID 页面包含以下字段：

➢ 本地引擎 ID（5~32 个字符）：显示了本地机器的识别号。此号用十六进制表示。每个字节由两个十六进制数。每个字节可以由空格和冒号格开。在使用 SNMP 版本 3 之前，机器识别号必须被定义。选择默认的机器识别号，它由企业号和默认物理地址组成。

➢ 用户默认：使用设备生成的引擎 ID。默认的引擎 ID 是基于设备的 MAC 地址和按以下标准定义的：

  – 头 4 个字节：第一个数据位为 1，其他的是 IANA 企业号码。

  – 第 1 个字节：设置为 3 用以指明后面跟随的是 MAC 地址。

  – 最后 6 个字节：设备的 MAC 地址。

2. 定义本地引擎 ID 和用户默认字段。

3. 点击“提交”。设置 SNMP 安全性全局参数，设备更新。

11.3.2 定义SNMP视图

SNMP 视图提供或阻止对设备的功能或者功能的一部分进行访问。比如，一个视图可以定义为提供 SNMP 组 A 只读访问组播组，同时提供 SNMP 组 B 可以读写访问组播组。特征访问是通过 MIB 名称或者 MIB 对象 ID 来实现的。

定义 SNMP 视图的步骤：

1. 点击：SNMP 管理>安全>视图，打开视图页面：



图 11-2 视图页面

视图页面包括以下字段：

- 视图名称：显示用户自定义视图，视图名称最多可填入 30 个字符。
- 对象 ID 子树：显示设备包括或者排除于指定的 SNMP 视图的特征对象 ID。
- 视图类型：指明所指定的对象 ID 子树是包括还是排除于所选的 SNMP 视图。
- 删除：删除当前选择的视图，可能的值包括：
  - 选中：删除所选的视图。
  - 不选中：保留视图列表。

2. 点击“创建”，打开添加 SNMP 视图页面：



图 11-3 添加 SNMP 视图页面

3. 定义视图名称字段。

4. 用“上”和“下”定义视图。

5. 定义视图类型字段。

6. 点击“提交”，视图被定义，设备更新。

11.3.3 定义SNMP组

SNMP 安全性组页面提供创建 SNMP 组信息，分配 SNMP 访问控制 SNMP 组特权。组允许网络管理者给特殊的设备功能分配访问权限。

定义 SNMP 组的步骤:

1. 点击：SNMP 管理>安全>组配置文件，打开 SNMP 组页面：



图 11-4 SNMP 组页面

SNMP 组页面包含以下字段：

- 组名：显示用户自定义访问规则的组。范围为 30 个字母。
- 安全模型：定义组所包含的 SNMP 版本，可能的值包括：
  - SNMPv1：SNMPv1 被定义到组。
  - SNMPv2c：SNMPv2c 被定义到组。
  - SNMPv3：SNMPv3 被定义到组。
- 安全等级：定义组的安全等级。安全等级只有在 SNMPv3 下才能被使用。可能的值包括：
  - 无认证：指定组没有认证也没有保密。
  - 认证：认证 SNMP 消息，并且保证对 SNMP 消息源进行认证。
  - 保密：将 SNMP 消息加密。
- 操作：定义组的访问权限。可能的值包括：
  - 读取：管理访问受到只读的限制，而且 SNMP 视图不能被改变。
  - 写入：管理访问可以读写，而且 SNMP 视图可以被改变。

– 通知：发送陷阱给指派的 SNMP 视图。

➢ 删除：删除 SNMP 组，可能的值包括：

– 选中：删除选择的 SNMP 组。

– 不选中：保留 SNMP 组。

2. 点击“创建”，打开添加 SNMP 组配置文件页面：



图 11-5 添加 SNMP 组配置文件页面

3. 定义组名，安全模型，安全等级和操作等字段。

4. 点击“提交”，添加 SNMP 组配置文件，设备更新。

修改 SNMP 组设置步骤：

1. 点击：SNMP 管理>安全>组配置文件，打开 SNMP 组页面。

2. 点击，打开 SNMP 组配置文件设置页面：



图 11-6 SNMP 组配置文件设置页面

3. 修改组名，安全模型，安全等级和操作字段。

4. 点击“提交”，修改 SNMP 组配置文件，设备更新。

11.3.4 定义SNMP组成员

SNMP 安全组成员页面允许将系统用户加入到 SNMP 组并定义对用户的认证方法。

定义组成员的步骤：

1. 点击：SNMP 管理>安全>组成员，打开 SNMP 安全组成员页面：



图 11-7 SNMP 安全组成员页面

SNMP 安全组成员页面包含以下字段：

- 用户名：包括一个用户自定义的用户名列表，范围为 30 个字符。
- 组名：包括一个用户自定义的 SNMP 组列表。SNMP 组在 SNMP 组配置文件页面被定义。
- 引擎 ID：显示本地或者远程的连接到用户的 SNMP 实体。改变或者删除本地 SNMP 引擎 ID 将会删除 SNMPv3 的用户数据。
  - 本地：指明用户连接到一个本地的 SNMP 实体。
  - 远程：指明用户连接到一个远程的 SNMP 实体，如果定义了引擎 ID，远程设备将会获得告知信息。
- 认证：显示认证用户所使用的认证方法，可能的值包括：
  - MD5 Key：用户使用 HMAC - MD5 算法来进行认证。
  - SHA Key：用户使用 HMAC - SHA - 96 认证级别来进行认证。
  - MD5 Password：使用 HMAC - MD5 - 96 密码进行认证。用户需要输入一个密码。
  - SHA Password：用户使用 HMAC - SHA - 96 认证级别来进行认证。用户需要输入一个密码。
  - 无：没有使用用户认证。
- 删除：从一个特定组里删除用户，可能的值包括：
  - 选中：删除所选的用户。
  - 不选中：保留用户列表。

2. 点击“创建”，打开添加 SNMP 组成员关系页面：



图 11-8 添加 SNMP 组成员关系页面

除了在 SNMP 安全组成员页面中包括的一些字段外，添加 SNMP 组成员关系页面还包含以下字段：

- 认证方法：定义 SNMP 的授权方法。
- 认证密钥：定义 HMAC-MD5-96 和 HMAC-SHA-96 的授权级别。添加授权和个人密钥来定义授权密钥。如果只要求授权一项，需要输入 16 个字节，如果个人密钥和授权两者都需要，则需要输入 32 个字节。十六进制字符串中的每个字节包括两个十六进制数，每个字节用空格或者冒号分开。
- 密码：定义组成员密码。

3. 定义用户名，引擎 ID，组名，认证方法，密码，认证密钥和保密密钥字段。

4. 点击“提交”，修改 SNMP 组成员关系，设备更新。

修改 SNMP 组成员设置步骤：

1. 点击：SNMP 管理>安全>组成员，打开用户页面。

2. 点击，打开 SNMP 组成员关系设置页面：

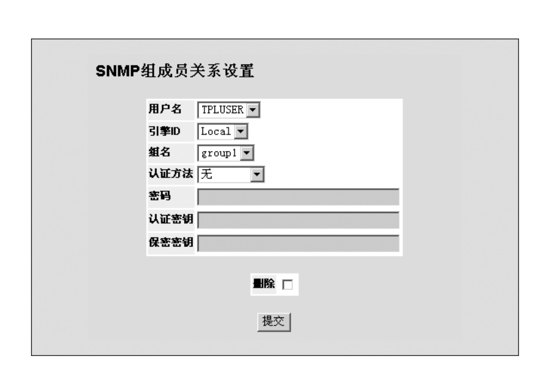


图 11-9 SNMP 组成员关系设置页面

3. 修改用户名，引擎 ID，组名，认证方法，密码，认证密钥和保密密钥字段。

4. 点击“提交”，修改 SNMP 组成员关系，设备更新。

11.3.5 定义SNMP团体

通过在 SNMP 团体页面中定义团体来管理访问权限。团体名称改变，访问权限也改变。SNMP 团体只能在 SNMP 版本 1 和版本 2c 定义。

定义 SNMP 团体的步骤：

1. 点击：SNMP 管理>安全>团体，打开 SNMP 安全团体页面：



图 11-10 SNMP 安全团体页面

SNMP 安全团体页面包含以下两项：

- SNMP 团体基本表
- SNMP 团体高级表

11.3.5.1 SNMP团体基本表

SNMP 团体基本表包含下列字段：

- 管理站点：显示定义了基本 SNMP 团体的管理站点的 IP 地址。
- 团体字符串：定义用于认证管理站点的密码。
- 访问模式：定义团体的访问权限，可能的值包括：
  - 只读：管理访问权限为只读，且不能对团体做任何改变。
  - 读写：管理访问权限为读写和改变设备的配置，但是不能对团体做出编辑。
  - SNMP 管理：用户拥有对设备的所有访问权限，包括允许更改团体。
- 视图名称：包括一个用户自定义的 SNMP 视图。
- 删除：删除一个团体，可能的值包括：
  - 选中：删除所选的 SNMP 团体。
  - 不选中：保留 SNMP 团体。

11.3.5.2 SNMP团体高级表

SNMP 团体高级表包含以下字段：

- 管理站点：显示定义了高级 SNMP 团体的管理站点的 IP 地址。
- 团体字符串：定义用于认证管理站点的密码。
- 组名：定义高级 SNMP 团体组名。
- 删除：删除一个团体，可能的值包括：
  - 选中：删除一个选择的 SNMP 团体。
  - 不选中：保留 SNMP 团体。

2. 点击“创建”，打开添加 SNMP 团体页面：



图 11-11 添加 SNMP 团体页面

3. 定义 SNMP 管理站点，团体字符串和基本或者高级字段。
4. 点击“提交”，添加 SNMP 团体，设备更新。

修改 SNMP 组成员设置步骤;

1. 点击：SNMP 管理>安全>团体。
2. 点击，打开 SNMP 团体设置页面：



图 11-12 SNMP 团体设置页面

3. 修改 SNMP 管理，团体字符串和基本或者高级字段。
4. 点击“提交”，修改 SNMP 团体，设备更新。

11.4 SNMP报告设置

这部分描述了 SNMP 报告的配置。包含以下主题：

- 定义 SNMP 报告属性
- 定义报告过滤
- 定义报告接收

11.4.1 定义SNMP报告属性

SNMP 报告属性页面包括定义 SNMP 报告参数。

定义 SNMP 报告全局参数：

1. 点击：SNMP 管理>报告>属性，打开全局陷阱设置页面：



图 11-13 全局陷阱设置页面

全局陷阱设置页面包括以下字段：

- 启用 SNMP 通知：定义设备是否发送 SNMP 通知。可能的值包括：
  - 选中：启用 SNMP 通知。
  - 不选中：禁用 SNMP 通知。
- 启用认证通知：定义设备是否启用认证失败通知。可能的值包括：
  - 选中：启用设备发送认证失败通知。
  - 不选中：禁止设备发送认证失败通知。

2. 定义启用 SNMP 通知和启用 SNMP 通知字段。

3. 点击“提交”，定义 SNMP 报告属性，设备更新。

11.4.2 定义报告过滤

SNMP 报告过滤页面允许过滤基于对象标识的陷阱。每个对象标识被连接到设备特征或者特征的一部分。SNMP 过滤页面同时允许网络管理者过滤报告。

定义报告过滤：

1. 点击：SNMP 管理>报告>通知过滤器，打开陷阱过滤设置页面：



图 11-14 陷阱过滤设置页面

陷阱过滤设置页面包括以下字段：

➢ 过滤器名：包括一个用户自定义的通知过滤器列表。

➢ 对象 ID 子树：显示发送或者阻止通知的对象 ID。如果一个对象 ID 包含了一个过滤器，就会产生和发送陷阱和通知到一个陷阱接收设备。对象 ID 可以从选择框中选择或者在对象 ID 框中填入。

➢ 过滤器类型：指明是否发送陷阱或者通知到选择的对象 ID。

  – 排除：不发送陷阱或者通知。

  – 包括：发送陷阱或者通知。

➢ 删除：删除过滤器。

  – 选中：删除选择的过滤器。

  – 不选中：保留过滤器列表。

2. 点击“创建”，打开添加 SNMP 通知过滤器页面：



图 11-15 添加 SNMP 通知过滤器页面

3. 定义过滤器名，新对象标识符树和过滤器类型字段。

4. 点击“提交”，定义 SNMP 报告过滤，设备更新。

11.4.3 定义报告接收

SNMP 报告接收页面包含陷阱接收用户及发送类型等过滤器设定信息。SNMP 报告过滤提供下列服务：

- 识别管理陷阱目标
- 陷阱过滤
- 选择陷阱产生参数
- 提供访问控制检查

定义 SNMP 报告过滤：

1. 点击：SNMP 管理>报告>通知接收器，打开陷阱站点管理页面：



图 11-16 陷阱站点管理页面

陷阱站点管理页面包含以下两项：

- SNMPv1,2 通知接收设备
- SNMPv3 通知接收设备

11.4.3.1 SNMPv1,2 通知接收设备

SNMPv1,2 通知接收设备包括下列字段：

- 接受设备 IP：显示陷阱发送的目的 IP。
- 通知类型：显示发送的通知的类型，可能的值包括：
  - 陷阱：指明发送的是陷阱。
  - 通知：指明发送的是通知。

- 团体字符串：显示陷阱管理器的团体字符串。
- 通知版本：显示陷阱类型，可能的值包括：
  - SNMP v1：指明发送的是 SNMP v1 陷阱。
  - SNMP v2c：指明发送的是 SNMP v2c 陷阱。
- UDP 端口号：显示发送通知所使用的 UDP 端口号，取值范围为 1 - 65535，默认值是 162。
- 过滤器名称：指明 SNMP 过滤是定义给哪一个 SNMP 通知过滤器。
- 超时：指明等待再次发送的时间，单位为秒，取值范围 1 - 300，默认值 15 秒。
- 重试：指明设备重新发送的次数，取值范围为 1 - 255，默认值是 3。
- 删除：删除所选择的接受器设备，可能的值包括：
  - 选中：从接受器设备列表里删除选择的接受器设备。
  - 不选中：保留接受器设备列表。

11.4.3.2 SNMPv3 通知接收设备

SNMPv3 通知接收设备包括下列字段：

- 接受设备 IP：显示陷阱发送的目的 IP。
- 通知类型：示发送的通知的类型，可能的值包括：
  - 陷阱：指明发送的是陷阱。
  - 通知：指明发送的是通知。
- 用户名：显示 SNMP 通知发送给的用户。
- 安全级别：显示数据包认证的情况，可能的值包括：
  - 未认证：指明数据包既没有认证也没有保密。
  - 认证：指明数据包已通过认证。
- UDP 端口号：显示发送通知所使用的 UDP 端口号，取值范围为 1 - 65535，默认值是 162。
- 过滤器名称：包括或者排除 SNMP 过滤。
- 超时：指明等待再次发送的时间，单位为秒，取值范围 1 - 300，默认值 15 秒。
- 重试：指明设备重新发送的次数，取值范围为 1 - 255，默认值是 3。
- 删除：删除所选择的接受器设备，可能的值包括：
  - 选中：从接受器设备列表里删除选择的接受器设备。

– 不选中：保留接受器设备列表。

2. 点击“创建”，打开添加 SNMP 通知接收设备页面：



图 11-17 添加 SNMP 通知接收设备页面

3. 定义接收设备 IP，通知类型，SNMPv1,2，SNMPv3，UDP 端口号，过滤器名，超时和重试字段。

4. 点击“提交”，定义 SNMP 通知接收器，设备更新。

修改 SNMP 通知接收器：

1. 点击：SNMP 管理>报告>通知接收器，打开陷阱站点管理页面。

2. 点击，打开 SNMP 通知接收设备设置页面：



图 11-18 SNMP 通知接收设备设置页面

3. 修改通知类型，SNMPv1,2，SNMPv3，UDP 端口号，过滤器名，超时和重试字段。

4. 点击“提交”，定义 SNMP 通知接收器，设备更新。

第12章 配置服务质量

本章包含以下主题：

- 服务质量概述
- 启用服务质量
- 队列映射

12.1 服务质量概述

网络流量常常是不可预知，唯一能提供的保证是尽最大可能去传输。为了克服这种挑战，服务质量（QoS）的应用贯穿于整个网络。这就保证了网络流量按照一个指定的标准来区分优先顺序，特定的流量接受优先处理。在网络中 QoS 优化网络性能并提供两个基本的特性：

- 基于以下的属性来将输入流量分类到操作的类中，包括：
  - 入接口
  - 包内容
  - 以上属性的结合
- 提供多种给不同的操作类分配网络资源的机制，包括：
  - 分配网络流量给特定的硬件队列
  - 内部资源分配
  - 流量修整

本文档中，术语服务等级（CoS）和服务质量（QoS）使用在以下语境中：

- CoS 提供多种 2 层流量服务。CoS 把流量分级提交到一个总的集合而不是为每个数据流分别设置的流量级中。CoS 常常与 802.1p 服务相关，该服务依据在 VLAN 头中设置的 2 层优先级来分级数据流。
- QoS 参考 2 层及 2 层以上的流量。QoS 处理每个数据流设置，甚至在同一个流量级中。
- QoS 特性包含以下元素：
- 流量分级 - 基于包内容和/或前后关系来把每个输入包按给定的流量级分级。
- 分配硬件队列 - 将输入包分配给转发队列。由分级机制定义的包所属的流量级的功能是将包发送给特定的队列处理。
- 流量分级-处理属性 - 应用 QoS/CoS 机制区分等级，包括：
  - 带宽管理

– 修整/速率限制

– 策略

12.1.1 映射到队列

在基本和高级 QoS 模式中都会用到队列。默认设置用于映射服务 QoS 模式。可以选择信任行为或输出服务字段，包括：

- VLAN 优先级标签（VPT） - VPT 基于 VPT 被映射到输出队列。而队列映射是用户自定义的，接下来是 VPT 默认映射到输出队列。在 VPT 默认映射中，队列 1 有最低的优先级。

下表包含 VPT 到队列的默认设置：

VPT 值	队列号
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

表 12-1 VPT 默认映射表

在系统范围基础上执行 VPT 到输出队列的映射，可以在每个端口上启用或禁用。

- 默认 CoS：到达的未标记的包被分配给默认的 VPT，该默认 VPT 可以由用户在每个端口上设置。一旦分配了 VPT，包就被看作到达时带有该标签。VPT 映射到输出队列是基于相同的用户自定义的以标签为基础定义的 802.1p.

- DSCP：用户可以用输出包到输出优先级队列的 IP DSCP 来配置系统。在每个系统基础上设置 IP DSCP 到优先级队列的映射。如果这种模式可用，无 IP 的包总是被归类到最大努力队列。

下表显示了默认的映射：

DSCP 值	队列号
0-15	q1 (最低等级)
16-31	q2
32-47	q3
48-64	q4

表 12-2 DSCP 默认映射表

所有未分配 DSCP 值的网络流量都将以最大努力服务转发。

包被分配一个指定队列后，通过使用所选择的分类方法可以应用多种服务。可以配置输出队列调度，包括：

- 精确优先级
- 加权轮流调度(WRR)

每个系统指定调度计划。可以以任意顺序给队列分配 WRR 权重。对每个接口或队列，可以配置以下输出流整形：

- 承诺突发量（CBS）
- 承诺信息率（CIR）
- 超过极限流量动作

12.1.2 QoS模式

设备支持以下 QoS 模式：

- 基本 QoS 模式
- 高级 QoS 模式

☞ 注意：

当在基本模式和高级模式之间切换时，可能会丢失一些设置。

12.1.2.1 基本QoS模式

基本模式支持激活以下信任设置中的一项：

- VLAN 点标签
- 差分服务码点
- 无

另外，单个基于 IP 的访问控制列表（ACL）可以直接附属在接口上（进一步信息可以查阅网络安全那节）。只有具有转发动作的包才被以基于指定的等级分配到输出队列。恰当配置输出队列，可以设置以下基本模式服务：

- 最低延迟 - 该队列被分配一个严格的优先级策略且流量被分配到最高优先级队列。
- 最好效果 - 流量被分配到最低优先级队列。
- 带宽分配 - 通过配置 WRR 调度计划和选择恰当的权重来分配带宽。

12.1.2.2 高级QoS模式

高级 QoS 模式提供为指定数据流的等级和与带宽管理相关的分配行为的规则。

在将包分配给指定的队列后，可以在每个端口上应用为调度计划配置输出队列，为突发尺寸配置修整，CIR，或 CBS 等服务。高级模式中，输出包可能带有异于预期的不同 VPT 标签。

12.2 启用服务质量

本节包含以下主题：

- 启用服务质量
- 定义队列

12.2.1 启用服务质量

CoS 设置页面包含启用或禁用 QoS 的字段。另外，可以选择信任模式。信任模式依赖于包中的预定义字段来决定输出队列设置。

启用 QoS 和定义基本设置：

1. 点击：QoS 服务质量>常规设置> CoS，打开 CoS 页面：

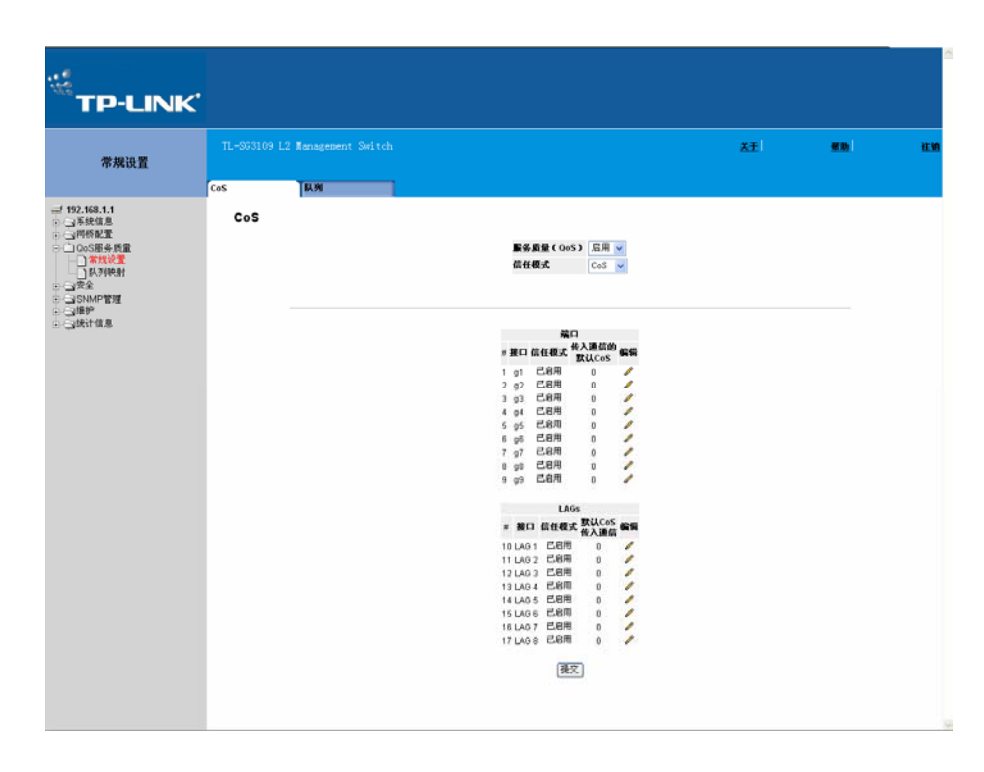


图 12-1 CoS 页面

CoS 页面包含以下字段：

- 服务质量（QoS）：表明是否在接口上启用 QoS。可能的值是：
  - 启用：在接口上启用 QoS。
  - 禁用：在接口上禁用 QoS。
- 信任模式：选择信任模式。如果数据包的 CoS 标签和 DSCP 标签被映射到不同的队列，信任模式决定数据包将被分配到哪个队列。可能的值是：
  - 无：未设置信任模式。所有的数据包被送往最低优先级队列。
  - CoS：设置信任模式为 CoS。数据包将被基于其 CoS 标签值排队。
  - DSCP：设置信任模式为 DSCP。数据包将被基于其 DSCP 标签值排队。

在端口列表中：

- #：表示为其定义了全局 QoS 参数的接口的编号。
- 接口：显示定义了全局 QoS 参数的接口的名字。
- 信任模式：显示是否在接口上启用了信任模式。
- 传入通信的默认 CoS：显示未定义 VLAN 标签的传入数据包的默认 CoS 值的当前设置。可能的值是 0-7。默认 CoS 是 0。

2. 在服务质量（QoS）字段选择启用。

3. 选择信任模式。

4.　点击“提交”，在设备上启用配置。

更改接口设置：

1.　点击✐，打开 CoS 设置页面：

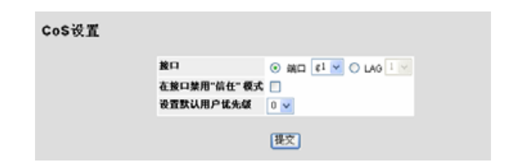


图 12-2 QoS 设置页面

2.　定义字段。

3.　点击“提交”，更新接口设置。

12.2.2 定义队列

QoS 队列设置页面包含定义 QoS 队列转发类型的字段。在系统级设置队列。

为服务质量定义队列设置：

1.　点击：QoS 服务质量>常规设置>队列，打开队列页面：



图 12-3 队列页面

队列页面包含以下字段：

- 严格优先级：表明选择的队列的流量调度严格基于队列的优先级。
- WRR：表明选择的队列的流量调度严格基于 WRR。

2.　定义各字段。

3.　点击“提交”，保存 QoS 队列设置和更新设备。

12.3 队列映射

本节包含以下主题：

- 映射 CoS 值到队列

➢ 映射 QoS 值到队列

12.3.1 映射CoS值到队列

CoS 到队列页面包含分级 CoS 设置到流量队列的字段。

设置 CoS 到队列：

1. 点击：QoS 服务质量>队列映射> CoS 到队列，打开 QoS 到队列页面：



图 12-4 QoS 到队列页面

CoS 到队列页面包含以下字段：

➢ 服务级别：指定 CoS 优先级标签值，该处 0 为最低 8 为最高。

➢ 队列：定义发送到映射了 CoS 优先级的队列的流量。支持四种流量优先级，0 的优先级最低，8 最高。

➢ 恢复默认设置：允许恢复默认设置。

2. 修改队列值或选择恢复默认值。

3. 点击“提交”，保存 CoS 到队列的映射设置并更新设备。

12.3.2 映射QoS值到队列

DSCP 到队列页面包含设置分级 DSCP 到流量队列的字段。例如，带 DSCP 标签值为 3 的包可以分配给队列 2。

设置 DSCP 到队列：

1. 点击：QoS 服务质量>队列映射> DSCP 到队列，打开 DSCP 优先级页面：



图 12-5 DSCP 优先级页面

DSCP 优先级页面包含以下字段：

➢ 接收包 DSCP 值：显示接收数据包的 DSCP 值。

➢ 队列：定义发送到队列的映射了 DSCP 优先级的流量。支持四种特殊优先级队列。

2. 修改队列值。

3. 点击“提交”，更新 DSCP 到队列的映射。

第13章　管理系统文件

设备上的文件维护包括配置文件的管理和设备的访问。配置文件由以下文件组成：

- 启动配置文件：包括设备关机、重起和重新配置设备的名字时的一些指令。启动文件是通过从当前运行的配置文件或者备份配置文件拷贝指令创建的。

- 当前运行配置文件：包括所有的配置文件指令，也包括当前输入的指令。当设备关机或者重新启动后，当前运行配置文件中的指令将会丢失。在重新启动时，启动配置文件中的所有指令被拷贝到当前配置文件并应用到设备。在操作过程中。所有新的指令都被添加到当前运行配置文件中。指令并不保存。在关闭设备之前，必须把当前配置文件的内容拷贝到启动配置文件中。下一次重新启动设备时，指令必须从启动配置文件中拷贝回当前运行配置文件中。

- 映像文件：下载新版本的文件更新软件。检查文件的格式正确。更新完成。成功下载后，将显示新的版本，重启设备将生效。

这部分包含以下主题：

- 下载系统文件
- 上传系统文件
- 使用映像文件
- 复制系统文件

13.1 下载系统文件

下载系统文件：

点击：维护>文件管理>文件下载，打开文件下载页面：



图 13-1 文件下载页面

文件下载页面分以下部分：

- 下载类型
- Firmware 下载
- 配置下载

13.1.1 下载类型

下载类型包含以下字段：

- Firmware 下载：描述了硬件下载的相关内容。当选择硬件下载时，配置下载框将变为灰色。
- 配置下载：描述了配置下载的相关内容。当选择硬件下载时，硬件下载框将变为灰色。

13.1.2 Firmware下载

Firmware 下载部分包含以下字段：

- TFTP 服务器 IP 地址：指定提供文件下载的 TFTP 服务器的地址。
- 源文件名：指定被下载文件的名字。
- 目标文件名：指定系统文件被下载到目标文件。可能有两种情况：
  - 软件映像：下载映像文件。
  - 引导代码：下载引导文件。

13.1.3 配置下载

1. 配置下载部分包含以下字段：

- TFTP 服务器 IP 地址：指定提供文件下载的 TFTP 服务器的地址。
- 源文件名：指定被下载文件的名字。
- 目标文件名：指定将下载配置文件的目标文件名。可能有两种情况：
  - 运行配置：下载指令到当前配置文件中。
  - 启动配置：下载新的启动配置文件，覆盖原有的启动文件。

2. 打开文件下载页面。
3. 选择下载类型。
4. 指定 TFTP 服务器 IP 地址。
5. 指定源文件名和目标文件位置。
6. 点击“提交”，需求的文件被下载到指定的目标。

13.2 上传系统文件

复制文件页面包括从设备上把软件上传到 TFTP 服务器。

上传文件：

点击：维护>文件管理>文件上传，打开文件上传页面：



图 13-2 文件上传页面

文件上传页面包括以下主题：

- 上传类型
- 软件文件上传
- 配置上传

13.2.1 上传类型

上传类型包含以下字段：

- Firmware 上传：描述了软件映像文件上传的情况。当选择硬件上传时，配置上传框将变为灰色。
- 配置上传：描述了配置文件上传的情况。当选择硬件上传时，硬件上传框将变为灰色。

13.2.2 软件文件上传

软件文件上传部分包含以下字段：

- TFTP 服务器 IP 地址：定义软件映像被上传到的 TFTP 服务器的地址。
- 目标文件名：定义被上传的软件映像的名字。

13.2.3 配置上传

1. 配置上传包含以下字段：

- TFTP 服务器 IP 地址：定义配置文件被上载到的 TFTP 服务器的地址。
- 目标文件名：定义启动文件被上载到的文件的名字。
- 传输文件名：定义被上载的配置文件的名字。有两种情况：
  - 运行配置：上载当前配置文件。
  - 启动配置：上载启动文件。

2. 打开复制文件页面。参照 13.4 节“复制系统文件”内容。
3. 定义上载文件的类型。
4. 指定上载区域。
5. 点击"提交"，软件被上载到设备。

13.3 使用映像文件

映像页面允许网络管理者选择和重新设置映像文件。

下载系统文件：

1. 点击：维护>文件管理>当前映像文件，打开活动映像页面：



图 13-3 活动映像页面

活动映像页面包含以下字段：

- 装置号：为映像文件进行选择的装置号。
- 当前映像文件：当前活动在装置上的映像文件。
- 复位之后：设备复位之后活动在装置上的映像文件。可能的值包括：

– 映像文件 1：在设备复位之后激活映像文件 1。

– 映像文件 2：在设备复位之后激活映像文件 2。

2. 选择映像文件。

3. 点击“提交”，设备重启后，被选择的映像文件起作用。

13.4 复制系统文件

在复制文件页面，文件能够被复制和删除。

复制系统文件：

1. 点击：维护>文件管理>复制文件，打开复制文件页面：



图 13-4 复制文件页面

复制文件页面包括以下字段：

- 复制配置：复制运行配置到启动配置文件上。
- 源：表明选定运行配置。
- 目的：表明选定启动配置。
- 恢复出厂默认配置：复位出厂默认配置。在设备复位恢复出厂默认值。此项不选中，则设备维持当前配置文件。

2. 选择复制配置字段。

3. 点击“提交”，文件被复制。

恢复出厂配置：

1. 点击：维护>文件管理>复制文件，打开复制文件页面。

2. 选择恢复出厂默认配置。

3. 点击“提交”，恢复出厂配置，设备更新。

第14章　设备诊断

本章包含以下主题：

- 配置端口镜像
- 查看所有电缆测试
- 查看光收发器

14.1 配置端口镜像

端口镜像功能就是拷贝一个端口接收和发送的数据包到监控端口，以此来监控和反映网络数据流。端口镜像可以作为诊断和调试工具，同时让交换机执行监控功能。网络管理员可以通过选择源端口与目的端口来完成端口镜像的配置。

执行端口镜像诊断：

1. 点击：维护>诊断>端口镜像，打开端口镜像页面：



图 14-1 端口镜像页面

端口镜像页面包含以下字段：

- 目的端口：定义进行数据交换的目标端口数。
- 源端口：指明对数据包进行镜像的端口。
- 类型：指明镜像端口模式配置。可能出现的情况如下：
  - 仅接收：定义接受端口的端口镜像。
  - 仅发送：定义进行数据交换的端口的端口镜像。
  - 接收和发送：定义接收端口和数据交换端口的端口镜像。此为默认信息。
- 状态：指明源端口当前的状态。
- 删除：删除端口镜像会话。可能出现的情况有：

– 选中：删除选定的端口镜像会话。

– 不选中：继续维持端口镜像会话。

2. 点击“创建”，打开添加端口镜像页面：

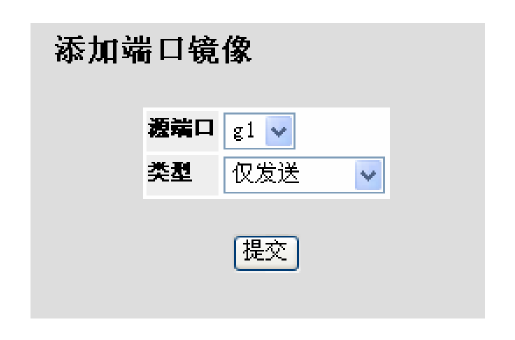


图 14-2 添加端口镜像页面

3. 在源端口字段选择一个端口。

4. 在类型字段选择一个端口类型。

5. 点击“提交”，提交端口会话定义，更新设备。

更改端口镜像设置：

1. 点击，打开端口镜像设置页面：

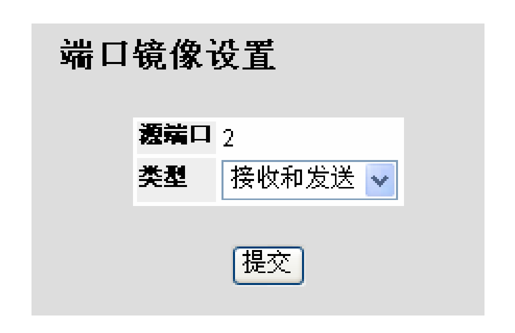


图 14-3 端口镜像设置页面

2. 修改类型字段。

3. 点击“提交”，提交端口镜像设置更改，更新设备。

清除端口镜像：

1. 点击：维护>诊断>端口镜像，打开端口镜像页面：

2. 在选择的条目上选中删除复选框并点击“提交”。

14.2 查看所有电缆测试

铜质电缆页面包含进行铜缆测试所需的信息。线缆测试将提供电缆出现错误的具体位置，最后一次进行测试的时间以及错误类型等信息。测试采用时域反射测量（TDR）技术，在源端口上对铜质电缆的质量和性能进行测试。可测试长度达 120 米。测试需在端口未连接状态下进行。

查看电缆测试结果：

1. 点击：维护>诊断>铜质电缆，打开铜质电缆页面：



图 14-4 铜质电缆页面

铜质电缆页面包含以下字段：

- 端口：具体指明线缆所连接的端口。
- 测试结果：显示电缆测试结果。可能出现以下情况：
  - No Cable：表明线缆尚未连接到端口。
  - Open Cable：表明线缆仅连接了一端。
  - Short Cable：表明线缆已发生短路。
  - OK：表明线缆已通过测试。
- 线缆故障距离：指明线缆出现错误的位置距端口的距离。
- 上一次更新：指明最后一次进行端口测试的时间。
- 线缆长度：指明线缆的近似长度。测试只有在端口 1Gbps 的连接状态下方能进行。

执行测试：

2. 点击“开始测试”，测试参数将显示在铜质电缆页面。

14.3 查看光收发器

光收发器页面允许网络管理员在光纤线路上执行测试。

☞ 注意：

只有当端口处于连接状态时才能执行光收发器诊断。

测试线缆：

1. 点击：维护>诊断>光收发器，打开光收发器页面：



图 14-5 光收发器页面

光收发器页面包含以下字段：

- 端口：显示所测试的线缆所在端口的 IP 地址。
- 温度：表明所操作的线缆温度（摄氏温度）。
- 电压：表明所操作的线缆电压。
- 电流：表明所操作的线缆电流。
- 电源输出：表明输出电源的传输率。
- 电源输入：表明输入电源的传输率。
- 发送故障：说明在传送过程中是否有错误发生。
- 信号损失：说明线缆上是否发生信号损失。
- 数据准备：表明收发器已达到通电状态，数据已准备完毕。

第15章　查看统计信息

这部分主要是描述如何查看和管理设备的接口统计、GVRP、EAP、以太网类的信息；以及说明如何查看和定义 RMON 的统计信息、历史记录、事件和警报。

这部分包括以下主题：

- 查看接口统计信息
- RMON 统计的管理

15.1 查看接口统计信息

这部分包含以下主题：

- 查看接口统计信息
- 查看以太网类统计信息
- 查看 GVRP 统计信息
- 查看 EAP 统计信息

15.1.1 查看接口统计信息

接口统计页面包括接收和发送包的统计。

查看接口统计信息：

1. 点击：统计信息>接口统计信息>接口，打开接口统计信息页面：



图 15-1 接口统计信息页面

接口统计信息页面包含以下字段：

- 接口：指明统计信息显示的设备。可能的值包括：
  - 端口：定义接口统计信息显示的接口
  - LAG：定义接口统计信息显示的 LAG
- 刷新频率：定义从上一次刷新起统计的时间，可能的值包括：
  - 15 秒：指明接口统计信息每 15 秒刷新一次
  - 30 秒：指明接口统计信息每 30 秒刷新一次
  - 60 秒：指明接口统计信息每 60 秒刷新一次
  - 不刷新：指明接口统计信息不刷新

接收统计信息

- 总字节：显示所选择的接口接收到的字节数。
- 单播包：显示所选择的接口接收到的单播包的数目。
- 组播包：显示所选择的接口接收到的组播包的数目。
- 广播包：显示所选择的接口接收到的广播包的数目。
- 错误包：显示所选择的接口接收到的错误包的数目。

发送统计信息

- 总字节：显示所选择的接口发送的字节数。
- 单播包：显示所选择的接口发送的单播包的数目。
- 组播包：显示所选择的接口发送的组播包的数目。
- 广播包：显示所选择的接口发送的广播包的数目。

2. 在接口字段选择一个端口，端口统计将会显示

清除接口统计数量

1. 打开接口统计信息页面。
2. 点击“清除所有计数”，接口统计的数量将会清除掉。

15.1.2 查看以太网类统计信息

以太网类统计信息页面包括接口统计信息。

查看以太网类信息统计：

1. 点击：统计信息>接口统计信息>以太网类，打开以太网类统计信息页面：



图 15-2 以太网类统计信息页面

以太网类统计信息页面包含以下字段：

- 接口：显示统计信息显示的设备。可能的值包括：
  - 端口：定义特定的端口进行以太网类统计。
  - LAG：定义特定的 LAG 进行以太网类统计。
- 刷新频率：定义从上一次接口统计刷新起通过的时间，可能的值包括：
  - 15 秒：指明以太网类统计信息每 15 秒刷新一次。
  - 30 秒：指明以太网类统计信息每 30 秒刷新一次。
  - 60 秒：指明以太网类统计信息每 60 秒刷新一次。
  - 不刷新：指明以太网类统计信息不刷新。
- FCS 错误：显示所选择的端口接收到的 FCS 错误的数目。
- 单碰撞帧：显示所选择的接口接收到的单碰撞帧的数目。
- 最近碰撞：显示所选择的接口最近接收到的碰撞帧的数目。
- Excessive Collisions：显示所选择的接口接收到的额外碰撞的数目。
- 超长包：显示所选择端口上超长包错误的数目。
- 内部 MAC 接收错误：显示所选择的端口内部 MAC 接收错误的数目。
- 收到的 Pause 帧：显示所选择接口接收到的 Pause 帧的数目。
- 发送的 Pause 帧：显示所选择接口发送的 Pause 帧的数目。

2. 在接口字段中选择一个接口（端口或 LAG），以太网类统计将会显示。

更新刷新时间：

➢ 变换统计刷新频率的方法只需从刷新频率下拉菜单中选择另一个刷新频率

复位以太网类统计信息的计数：

1. 打开以太网类统计信息页面。

2. 点击“清除所有计数”，以太网类统计数量将会清除。

15.1.3 查看GVRP统计信息

GVRP 统计信息页面包括为 GVRP 的设备统计信息。

查看 GVRP 统计信息：

1. 点击：统计信息>接口统计信息>GVRP，打开 GVRP 统计信息页面：



图 15-3 GVRP 统计信息页面

GVRP 统计信息页面包含以下字段：

➢ 接口：显示特定的接口类型的统计信息。

– 端口：指明显示端口的统计信息。

– LAG：指明显示 LAG 的统计信息。

➢ 刷新频率：指明 GVRP 统计信息刷新间隔的时间，可能的值包括：

– 15 秒：指明 GVRP 统计信息每 15 秒刷新一次。

– 30 秒：指明 GVRP 统计信息每 30 秒刷新一次。

– 60 秒：指明 GVRP 统计信息每 60 秒刷新一次。

– 不刷新：指明 GVRP 统计信息不刷新。

- 加入空：显示设备 GVRP 加入空的统计信息。
- 空：显示设备 GVRP 空的统计信息。
- 保留空：显示设备 GVRP 保留空的统计信息。
- 加入：显示设备 GVRP 加入的统计信息。
- 保留：显示设备 GVRP 保留的统计信息。
- 全部离开：显示设备 GVRP 全部离开的统计信息。
- 无效协议 ID：显示设备 GVRP 无效协议 ID 的统计信息。
- 无效属性类型：显示设备 GVRP 无效属性类型的统计信息。
- 无效属性值：显示设备 GVRP 无效属性值的统计信息。
- 无效属性长度：显示设备 GVRP 无效的属性长度的统计信息。
- 无效事件：显示设备 GVRP 无效事件的统计信息。

2. 在接口字段中选择一个接口（端口或 LAG），GVRP 统计信息将会显示。

更新刷新频率：

- 变换统计刷新频率的方法只需从刷新频率下拉菜单中选择另一个刷新频率。

复位 GVRP 接口统计的计数：

1. 打开 GVRP 统计信息页面。
2. 点击“清除所有计数”，GVRP 统计数量将会清除。

15.1.4 查看EAP统计信息

EAP 统计信息页面包括被定义端口上收到 EAP 包的相关信息。

查看 EAP 统计信息：

1. 点击：统计信息>接口统计信息>EAP，打开统计信息页面：



图 15-4 统计信息页面

统计信息页面包含以下字段：

➢ 端口：指明进行统计的端口。

➢ 刷新频率：指明从最后一次刷新起统计的时间，可能的值包括：

– 15 秒：指明 EPA 统计信息每 15 秒刷新一次。

– 30 秒：指明 EPA 统计信息每 30 秒刷新一次。

– 60 秒：指明 EPA 统计信息每 60 秒刷新一次。

– 不刷新：指明 EPA 统计信息不刷新。

➢ 帧接收：指明在端口接收到的有效的 EAPOL 帧的数目。

➢ 帧发送：指明通过端口发送的 EAPOL 帧的数目。

➢ 开始帧接收：指明在端口接收的 EAPOL 开始帧的数目。

➢ 注销帧接收：指明在端口接收的 EAPOL 注销帧的数目。

➢ 响应 ID 帧接收：指明在端口接收的 EAP 响应 ID 帧的数目。

➢ 响应帧接收：指明端口接收到的 EAP 响应帧的数目。

➢ 请求 ID 帧发送：指明在端口发送的请求 EAP 请求 ID 帧的数目。

➢ 请求帧发送：指明通过端口发送的 EPA 请求帧的数目。

➢ 无效帧接收：指明在端口接收到的无效的 EAPOL 帧的数目。

➢ 长度错误帧接收：指明在端口接收到的长度错误的 EAPOL 帧的数目。

➢ 最后的帧形式：指明最后接收到的帧包含的协议。

➢ 最后的帧来源：指明最后接收到的帧所包含的源 MAC 地址。

2. 在端口字段中选择一个端口，端口统计将会显示。

更新刷新时间：

➢ 变换统计刷新频率的方法只需从刷新频率下拉菜单中选择另一个刷新频率。

15.2 RMON统计的管理

这部分描述如何查看或管理网络上远程监控的统计、历史事件和警报。

这部分包含以下主题：

➢ 查看 RMON 统计信息

➢ 配置 RMON 历史记录

➢ 配置 RMON 事件

➢ 定义 RMON 警报

15.2.1 查看RMON统计信息

RMON 统计信息包括设备的利用信息和设备上发生过的错误。

查看 RMON 信息统计：

1. 点击：统计信息>RMON>统计信息，打开统计信息页面：



图 15-5 统计信息页面

统计信息页面包含以下字段：

➢ 接口：指出设备被统计的信息种类，可能的值包括：

- 端口：定义特定的端口显示 RMON 统计信息。
- LAG：定义特定的 LAG 显示 RMON 统计信息。

➢ 刷新频率：定义刷新的时间间隔。

- 15 秒：RMON 统计信息每 15 秒刷新一次。
- 30 秒：RMON 统计信息每 30 秒刷新一次。
- 60 秒：RMON 统计信息每 60 秒刷新一次。
- 不刷新：指明 RMON 统计信息不刷新。

➢ 接收字节：显示从上一次刷新到现在接口接收的字节数。这个数目包括错误包和 FCS 字段，但是不包括分割位。

➢ 接收包：显示从上一次刷新到现在接口接收的数据包数。包括错误包，广播包和组播包。

➢ 广播包：显示从上一次刷新到现在接口接收的正确的广播包数。

➢ 组播包：显示从上一次刷新到现在接口接收的正确的组播包数。

➢ CRC 校验错误：显示从上一次刷新到现在接口上发生的 CRC 校验错误数。

➢ 过小包：显示从上一次刷新到现在接口接收的过小包（小于 64 字节）数。

➢ 超长包：显示从上一次刷新到现在接口接收的超长包（大于 1518 字节）数。

➢ 碎片：显示从上一次刷新到现在接口接收的碎片（小于 64 字节的包，不包括分割位，但是包括 FCS 字段）数。

➢ 无用信息：显示接收到大于 1518 字节的包的总数，不包括分割位，但是包括所有的 FCS 字段。检测无用信息的范围在 20ms 到 150ms 之间。

➢ 碰撞：显示从上一次刷新到现在接口接收的碰撞数。

➢ xx 字节帧：显示从上一次刷新到现在接口接收的指定大小的帧的数量。

2. 在接口字段中选择一个接口（端口或 LAG），RMON 统计将会显示。

更新刷新时间：

➢ 变换统计刷新频率的方法只需从刷新频率下拉菜单中选择另一个刷新频率。

复位 RMON 统计信息的计数：

1. 打开统计信息页面。
2. 点击“清除所有计数”，RMON 统计数量将会清除。

15.2.2 配置RMON历史记录

这部分包含以下主题：

- 定义 RMON 历史记录控制
- 查看 RMON 历史记录表

15.2.2.1 定义RMON历史记录控制

历史记录控制页面包含从端口上采样数据的信息，例如，样本可以包括接口定义或流量检测周期。

设置 RMON 历史记录控制：

1. 点击：统计信息>RMON>历史记录>历史记录控制，打开历史记录控制页面：



图 15-6 历史记录控制页面

历史记录控制页面包含以下字段：

- 历史记录条目号：显示历史记录控制表的条目号。
- 源接口：显示取样的的接口，可能的值包括：
  - 端口：RMON 信息取样的特定端口。
  - LAG：RMON 信息取样的特定 LAG。
- 取样间隔：定义端口取样的间隔，单位为秒，取值范围为 1 - 3600。默认值为 1800 秒（等于 30 分钟）。
- 取样请求：显示保存的样例数。取值范围为 1 - 65535。默认值为 50。
- 当前取样数量：显示当前的取样数量。
- 所有者：显示请求 RMON 信息的 RMON 站点或者用户，可以填入 0 - 20 个字母。
- 删除：删除历史记录控制条目。可能的值包括：
  - 选中：删除选择的历史记录控制条目。

– 不选中：保留当前的历史记录控制条目。

2. 点击“创建”，打开添加历史记录条目页面：



图 15-7 添加历史记录条目页面

3. 设定每个字段。

4. 点击“提交”，实体将会增加到历史记录控制页面中，并且设备将会更新。

修改历史记录控制设置

1. 打开历史记录控制页面。

2. 点击，打开历史记录控制设置页面：

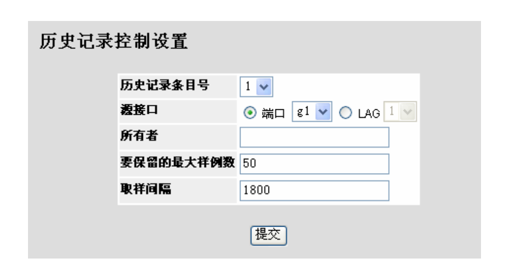


图 15-8 历史记录控制设置页面

3. 设定每个字段。

4. 点击“提交”，实体将会添加到历史记录控制页面中，并且设备将会更新。

15.2.2.2 查看RMON历史记录表

历史记录表页面包括端口详细的统计网络采样，每张实体表在每一次单采样时都会完成所有值的显示。

查看 RMON 历史记录表

1. 点击：统计信息>RMON>历史记录>历史记录表，打开历史记录表页面：



图 15-9 历史记录表页面

历史记录表页面包含以下字段：

- 历史记录条目号：显示历史记录控制表的条目号。
- 所有者：请求 RMON 信息的 RMON 站点或者用户。长度为 0 - 20 个字母。
- 样例号：指明状态统计的样例号码。
- 丢弃事件：显示从上一次刷新到现在接口丢弃事件出现的次数。
- 接受字节：显示从上一次刷新到现在接口接收的字节数。这个数目包括错误包和 FCS 字段，但是不包括分割位。
- 接收包：显示从上一次刷新到现在接口接收的数据包数。包括错误包，广播包和组播包。
- 广播包：显示从上一次刷新到现在接口接收的正确的广播包数。不包括组播包。
- 组播包：显示从上一次刷新到现在接口接收的正确的组播包数。
- CRC 校验错误：显示从上一次刷新到现在接口上发生的 CRC 校验错误数。
- 过小包：显示从上一次刷新到现在接口接收的过小包（小于 64 字节）数目。
- 超长包：显示从上一次刷新到现在接口接收的超长包（大于 1518 字节）数目。
- 碎片：显示从上一次刷新到现在接口接收的碎片（小于 64 字节的包，不包括分割位，但是包括 FCS 字段）的数目。
- 无用信息：显示接收到大于 1518 字节的包的总数，不包括分割位，但是包括所有的 FCS 字段。检测无用信息的范围在 20ms 到 150ms 之间。
- 碰撞：显示从上一次刷新到现在接口接收的碰撞数目。
- 使用：显示接口的使用率。

2. 在历史记录条目号中选择一个实体。

3. 点击“提交”，统计将会显示。

15.2.3 配置RMON事件

这部分包含以下主题：

- ➢ 设置 RMON 事件控制
- ➢ 查看 RMON 事件日志

15.2.3.1 设置RMON事件控制

事件控制页面包括 RMON 事件控制所有相关信息。

设置 RMON 事件控制

1. 点击：统计信息>RMON>事件>事件控制，打开事件控制页面：



图 15-10 事件控制页面

事件控制页面包含以下字段：

- ➢ 事件条目：显示的事件。
- ➢ 团体：显示事件所属的团体。
- ➢ 说明：显示用户定义的事件说明。
- ➢ 类型：描述事件的类型，可能的值包括：
  - – 日志：指明事件是一个日志条目。
  - – 陷阱：指明事件是一个陷阱。
  - – 日志和陷阱：指明事件同时是日至条目和陷阱。
  - – 无：指明没有事件产生。
- ➢ 时间：显示事件产生的时间。
- ➢ 所有者：显示定义事件的设备和用户。
- ➢ 删除：删除一个 RMON 事件。可能的值包括：

– 选中：删除一个选择的 RMON 事件。

– 不选中：保留 RMON 事件。

2. 点击“创建”，打开添加事件条目页面：



图 15-11 添加事件条目页面

3. 设定每个字段。

4. 点击“提交”，事件将会添加到事件控制页面中，并且设备将会更新。

修改 RMON 事件用户

1. 点击：统计信息>RMON>事件>事件控制，事件控制页面将会打开，显示定义实体的页面。

2. 点击，打开事件控制设置页面：



图 15-12 事件控制设置页面

3. 设定每个字段。

4. 点击“提交”，事件将会添加到事件控制页面中，并且设备将会更新。

15.2.3.2 查看RMON事件日志

事件日志页面包括一个 RMON 事件的表单。

查看 RMON 事件日志：

1. 点击：统计信息>RMON>事件>事件日志，打开事件日志页面：



图 15-13 事件日志页面

事件日志页面包含以下字段：

- 事件：显示 RMON 事件日志的条目号。
- 日志号：显示日志号码。
- 日志时间：显示日志条目记录的时间。
- 说明：显示日志条目的说明。

15.2.4 定义RMON警报

RMON 警报页面包括设置网络警报方面的信息，当一个网络问题或事件被检测时将发生警报。上升和下降阈值将触发警报。

定义 RMON 警报：

1. 点击：统计信息>RMON>警报，打开 RMON 警报页面：



图 15-14 RMON 警报页面

RMON 警报页面包含以下字段：

- 警报条目：指定一条警报。
- 计数器名：显示选择的 MIB 变量。
- 接口：显示被 RMON 统计的接口。

– 端口：显示被选择的端口的 RMON 统计信息。

– LAG：显示被选择的 LAG 的 RMON 统计信息。

➢ 计数器值：显示选择的 MIB 变量的值。

➢ 样例类型：为选择的变量定义取样的方法，再将取样的值与阈值进行比较。可能的值包括：

– 增量：将现在值减去上一次取样值之后的增量与阈值进行比较。

– 绝对：在一个取样周期结束时将取样结果直接与阈值进行比较。

➢ 上升阈值：显示触发警报的上升阈值的值。上升阈值出现在图表栏的顶端。每一个监控的变量将被指派一个不同的颜色。

➢ 上升事件：显示警报报告的机制，可能的值包括：

– 日志：指定对设备或者管理系统不使用保存机制，如果设备没有被复位，条目将会被保留在 LOG 表。

– 陷阱：指定使用 SNMP 陷阱，将通过陷阱机制发送。而且陷阱也是可以使用陷阱机制保存的。

– 两者：指定同时使用 LOG 和 TRAP 两种警报报告机制。

➢ 下降阈值：显示触发警报的下降阈值的值。下降阈值出现在图表栏的顶端。每一个监控的变量将被指派一个不同的颜色。

➢ 下降事件：显示警报报告的机制。

➢ 启动警报：显示警报触发的方式，上升被定为从一个低阈值上升到一个高阈值。

➢ 时间间隔（秒）：定义警报的时间间隔，以秒为单位。

➢ 所有者：显示定义警报的设备或者用户。

➢ 删除：删除 RMON 警报表条目。

2. 点击“创建”，打开添加警报条目页面：



图 15-15 添加警报条目页面

3. 设定各字段。

4. 点击“提交”，条目将会添加到 RMON 警报页面中，并且设备将会更新。

修改 RMON 警报条目

1. 点击✎，打开 RMON 警报设置页面：



图 15-16 RMON 警报设置页面

2. 修改各字段。

3. 点击“提交”，条目将会添加到 RMON 警报页面中，并且设备将会更新。

附录 术语表

术语表中包含本手册中常见名词短语的定义或描述，以英文字母顺序排序。

英文术语	中文对应术语	定义或描述
A		
Access Mode	访问模式	定义系统授权的用户访问模式。
Access Profile	访问配置文件	允许网络管理员定义访问设备配置文件和规则。可对按照以下准则定义的用户组授予受限的管理功能 访问权限： • 输入接口 • 源 IP 地址/源 IP 子网
ACE (Access Control Entry)	访问控制条目	访问控制列表中用来决定哪些网络流量被转发的过滤器。ACE 基于以下准则： • 协议 • 协议 ID • 源端口 • 目的端口 • 通配符掩码 • 源 IP 地址 • 目的 IP 地址
ACL	访问控制列表	访问控制列表可用来授权、拒绝、限制访问设备、特性或应用。
Aggregated VLAN	聚合 VLAN	将几个 VLAN 组合成一个聚合 VLAN。聚合 VLAN 能使路由器响应属于相同超级 VLAN 网的不同子 VLAN 网节点的 ARP 请求。路由器以它们的 MAC 地址来响应。
AHP (Authentication Header Protocol)	认证头协议	提供源主机认证和数据完整性。
ARP (Address Resolution Protocol)	地址解析协议	一种把 IP 地址转换成物理地址的协议。
ASIC (Application Specific Integrated Circuit)	专用集成电路	为某种应用专门设计的芯片。
Asset Tag	资产标签	指用户定义的设备描述。
Authentication Profile	认证配置文件	一组在登录时对用户和应用进行认证的规则。
Auto-negotiation	自动协商	允许 10/100Mps 或 10/100/1000Mbps 以太网端口建立如下特性： • 全双工/半双工模式 • 流控 • 速度
B		
Back Pressure	背压	在半双工模式时，用来使某个端口不接收数据包的一种机制。

Backbone	骨干网	一个网络的主干部分。骨干网类型包括： • 楼宇网 • 校园网 • 城域网 • 国内数据网 • 电信网
Backplane	背板	在设备内部传输信息的主要总线。
Bandwidth	带宽	在单位时间内传输数据的总量。对数字设备而言，带宽是指每秒传输的位数或每秒传输的字节数。
Bandwidth Assignment	带宽分配	指某个应用、用户或者接口分配到的带宽量。
Baud	波特	每秒钟传输信号码元的数量。
Best Effort	尽力服务	指流量被分配给最低的优先级队列、传输不能得到保证。
BGP (Border Gateway Protocol)	边界网关协议	使信息能够共享，在路由器组中路由信息。
Boot Version	引导版本	指引导程序的版本。
BootP (Bootstrap Protocol)	引导协议	使工作站能够发现它的 IP 地址，网络上引导服务器的 IP 地址，或者能够装载到引导设备的配置文件。
BPDU (Bridge Protocol Data Unit)	桥协议数据单元	在包格式里提供桥接信息，BPDU 在交换传输中携带生成树配置的信息。BPDU 包中的信息包含端口、地址、优先级和转发开销。
Bridge	网桥	连接两个不同网络的一种设备。网桥与硬件有关， 但是独立于协议。网桥工作在第一层和第二层。
Broadcast Domain	广播域	可接收指定集合内任意设备发出的广播帧的设备集合。路由器能够限制广播域，是因为路由器不转发广播包。
Broadcast Storm	广播风暴	通过一个单端口在网络上同时发送过量广播帧。转发信息的响应在网络中将会堆积起来，消耗过多的网络资源或造成网络超时。
Broadcasting	广播	向所有端口中发送数据包的方法。
Burst	突发	一个包以超过正常速率传输。突发是被限制的，并且只能在一定条件下才会发生。
Burst Size	突发长度	指以超出正常速率传输的数据量的大小。
C		
CBS (Committed Burst Size)	承诺突发量	QoS 输出流量整形的一种配置，指在一定时间间隔（承诺速率测量时间间隔）里允许传输最大数据量。
CDB (Configuration Data Base)	配置数据库	包含设备配置信息的一个文件。
CIDR (Classless Inter-Domain Routing)	无类别域间路由	基于路由的聚合，几个路由器一起组合成路由组，减少核心路由器携带的信息量，几个 IP 网络作为一个单一的更大的实体出现在组外的网络上。

CIR (Committed Information Rate)	承诺信息速率	QoS 输出流量整形的一种配置，指使用帧中继服务传输的数据速率。这个速率是在一定时间间隔（承诺速率测量时间间隔）里测量到的速率的平均值。
Class Map	类别映射图	一种由 IP ACL 和 MAC ACL 组成的 QoS 系统实现。类别映射图被配置为匹配包准则，并按照最先匹配的方式对包进行匹配。
Class of Service	服务类别	即 802.1p 优先级方案。CoS 提供了为数据包加入优先级标签的方法，即在数据包的 2 层包头上加入 0-7 的优先级字段，0 表示最低优先级，7 表示最高优先级。
CLI (Command Line Interface)	命令行接口	用来配置系统的一组命令集合。
Client	客户端	在其他计算机（通常称为服务器）上请求服务或者处理的计算机或程序。
CLL (Classification Control List)	分类控制列表	授权、拒绝、限制访问 QoS 中的设备、特性或应用的设备。
Collision	碰撞	重叠传送的两个或更多数据包发生碰撞。传送的数据不能被使用，会话也将重新开始。
Combo Port	Combo 端口	同一个逻辑端口具有两个物理连接，包括一个 RJ-45 连接和一个 SFP 连接。
Community	团体	一组具有相同访问权限的用户组成的用户组。
CPU (Central Processing Unit)	中央处理器	计算机内处理信息的部件。CPU 由控制单元和算术逻辑单元（ALU）组成。
D		
Damp	抑制	指一个端口因为翻动而不向相邻端口广播连接的状态。
DHCP (Dynamic Host Configuration Protocol)	动态主机配置协议	DHCP 可以动态地在一个网络上分配 IP 地址。使用动态 IP 地址，一个设备每次可以用不同的 IP 地址连接网络。DHCP 也支持混合的静态 IP 地址和动态 IP 地址。
DHCP Client	DHCP 客户端	网络上使用 DHCP 获得网络地址等配置参数的主机。
DHCP Server	DHCP 服务器	网络上给 DHCP 客户端返回配置参数的主机。
Domain	域	网络上按照共有规则组合起来的一组计算机或者设备。
DSCP (DiffServe Code Point)	差分服务代码点	DSCP 给 IP 包使用的一种优先级标签。
DSL (Digital Subscriber Line)	数字用户线路	DSL 提升了电话线传输数据的容量。
Duplex Mode	双工模式	在两个方向上都允许发送和接收数据，有两种不同类型的双工模式： • 全双工模式 – 允许同步的双向传输。比如电话，通话的双方可以同时传输和接收信息。 • 半双工模式 – 允许非同步的双向传输。比如对讲 机，一个时刻只允许一方传输信息。
DVMRP (Distance Vector Multicast Routing Protocol)	距离向量组播 路由协议	DVMRP 隧道以单播包进行组播。DVMRP 支持基于目的地址的速率限制和分布。

E		
Egress Port	输出端口	网络数据流从上面发送出来的端口。
EIGRP (Enhanced Interior Gateway Routing Protocol)	增强型内部网关路由协议	增强型内部网关路由协议提供快速聚合，支持可变长度的子网掩码，及支持多层网络层协议。
End System	终端系统	网络上的终端用户设备。
EPG (Exterior Gateway Protocol)	外部网关协议	外部网关协议在一个自治系统网络中允许相邻网关相互交换路由信息的协议。
ESP (Encapsulating Security Payload)	封装安全有效载荷	封装安全有效载荷为 IPv4 和 IPv6 提供多种安全服务。
Ethernet	以太网	以太网使用总线形或星形拓扑且支持的传输速率达到 10Mbps 数量级。称为快速以太网的新版本速率可达 100Mbps。以太网遵行 IEEE 802.3 标准。以太网是最普遍使用的局域网标准。
EWS (Embedded Web Server)	内置 Web 服务器	内置 Web 服务器提供通过标准 Web 浏览器管理设备的服务。内置 Web 服务器是命令行接口（CLI）和网络管理系统（NMS）的附加或替代功能。
F		
FE (Fast Ethernet)	快速以太网	快速以太网以 100Mbps 而非 10Mbps 的速率传输数据。
FFT (Fast Forward Table)	快速转发表	快速转发表提供关于转发路由的信息。假如包到达一个不知道路径的设备时，它经过在 FFT 中的路径转发包；而如果知道路径时，CPU 直接转发包并更新 FFT。
FIFO (First In First Out)	先进先出	队列处理时按照先进入队列中的包先被传输。
Flapping	翻动	描述一个串行接口开闭的术语，当一个接口的状态经常改变时就会发生翻动。例如，一个生成树（STP）端口经常从监听状态变换到学习转发状态。这个可能会引起有害的传输丢失。
Flow Control	流控	流控使低速设备能够和高速设备通讯。这种流控是通过高速设备重复发送包实现。
Fragment	片断	少于 576 比特的以太网数据包。
Frame	帧	一个含有物理介质层所需的头和尾信息的数据包。
FTP (File Transfer Protocol)	文件传输协议	在网络节点间传送文件。
G		
GARP (General Attributes Registration Protocol)	通用属性注册协议	将客户端工作站注册到组播域中。
GBIC (Gigabit Interface Converter)	千兆接口转换器	一个用于将网络设备连接到光纤传输系统里硬件模块。GBIC 把串行的电信号转换成串行的光信号或反之。
Gigabit Ethernet	千兆以太网	千兆以太网以 1000Mbps 的速率传输。它同时兼容 10/100Mbps 以太网标准。

GRE (Generic Routing Encapsulation)	通用路由封装	封装各种协议类型的包来实现隧道传输。GRE 创建一个到远程 IP 路由器的点对点虚拟连接。
GVRP (GARP VLAN Registration Protocol)	GARP VLAN 注册协议	GARP VLAN 注册协议将客户端工作站注册到 VLAN 中。
H		
HMP (Host Monitoring Protocol)	主机监控协议	从各种网络主机收集网络信息。HMP 既能监控遍布在 Internet 上的主机，又能监控单个网络中的主机。
HOL (Head of Line)	线端	数据包是排队的，在队列前头（即线端）的包比在队列结尾的包要早发送。
Hop	跳跃	两个网络设备（比如两个路由器）之间的通路。
Host	主机	一台提供信息源或服务其他计算机的计算机。
Hot Swapping	热插拔	当设备正在运行时允许特定模块被取掉和/或替换，且不需要重新配置设备。
HTTP (HyperText Transport Protocol)	超文本传输协议	超文本传输协议用于在 Internet 上的服务器和客户端之间传输 HTML 文件。
I		
IAD (Integrated Access Device)	集成接入设备	集成接入设备能够将多样的通讯技术复用到一条电话线路上进行传输。
IC (Integrated Circuit)	集成电路	用半导体材料制造的小尺寸电子元件。
ICMP (Internet Control Message Protocol)	Internet 控制信息协议	Internet 控制信息协议使得网关或目的主机可以与源主机通信，比如报告一个处理出错信息。
IDRP (Inter-Domain Routing Protocol)	域间路由协议	域间路由协议指定路由器如何与其他不同域路由器进行通信。
IEEE (Institute of Electrical and Electronics Engineers)	（美国）电气与电子工程师协会	开发通信与网络标准的工程组织。
IEEE 802.1d		用于生成树协议，IEEE 802.1d 支持 MAC 桥接以避免网络环路。
IEEE 802.1p		在数据链路层的介质访问控制子层上对网络流量加入优先级。
IEEE 802.1q		定义 VLAN 桥的操作。在桥式局域网结构中允许对 VLAN 的管理、定义和操作。
IGMP (Internet Group Management Protocol)	Internet 组管理协议	允许主机通知本地的交换机或路由器它想接收特定组播组的数据包。
IGP (Interior Gateway Protocol)	内部网关协议	内部网关协议允许一个自治网络内部的网关之间交换路由信息。

Image File	映像文件	系统程序映像保存在名为 image-1 和 image-2 的两个闪存区域中。活动映像保存活动的版本；另一个映像保存备用版本。
Ingress Port	输入端口	从上面接收到网络流量的端口。
IP (Internet Protocol)	Internet 协议	定义数据包的格式和寻址方法。IP 给数据包加上地址，并转发到正确的端口上。
IP Address	IP 地址	为连接到两个或多个 LAN 或 WAN 的网络设备分配的唯一地址。
IP Multicast	IP 组播	在一个网络中发送组播包，组播路由拷贝一个包到几个端口上。
IPv6 (IP version 6)	IP 版本 6	IPv4 升级产生的一个 Internet 协议的新版本。IPv6 把 IP 地址长度从 32 比特增加到 128 比特。此外 IPv6 支持更多层次的寻址，更多的可地址节点且支持更简单的自动地址配置。
IPX (Internetwork Packet Exchange)	网际数据包交换	实现无连接的通信。
J		
Jumbo Frame	超长帧	超长帧能用较少的帧数传输相同的数据，从而减少了非有效载荷的开销，降低了处理时间，确保更少的中断。
K		
Key Chain	密钥链	分配给端口的一组 MD5 密钥。密钥链是作为 RIP 或者 OSPF 的接口参数分配给端口的。
L		
L2TP (Layer 2 Tunnel Protocol)	二层隧道协议	帮助在拨号接入网络上建立虚拟专用网络，并且提供二层转发（L2F）协议和点对点隧道协议（PPTP）。
LAG (Link Aggregated Group)	链路聚合组	将多个端口或 VLAN 聚合成一个虚拟端口或 VLAN。
LAN （Local Area Network)	局域网	覆盖范围在单独房间、建筑物、校园或其它有限地理范围的网络。
Layer 2	二层	指 OSI 的七层网络模型中的第二层，即数据链路层。包括客户机或服务器的物理地址，由于有较少的信息要处理，第二层的处理速度比第三层快。
Layer 3	三层	指 OSI 的七层网络模型中的第三层，即网络层。包括逻辑地址和协议类型（IP、IPX 等）。基于包信息，如源地址和目的地址，第三层流量可以被加入优先级并被转发。由于有更多的信息要处理，第三层处理时间相比第二层要长。
Layer 4	四层	指 OSI 的七层网络模型中的第四层，即传输层。建立连接并且保证所有的数据到达正确的目的端。数据包在第四层的分析和转发取决于应用程序。
LCP (Link Control Protocol)	链路控制协议	链路控制协议管理认证、压缩和加密。

Load Balancing	负载均衡	将需要处理的数据平均分配到可用的网络资源上。例如，负载均衡可以将输入的数据包平均分配给所有的服务器，或者是将数据包重定向到下一个可用服务器。
M		
MAC Address (Media Access Control Address)	介质访问控制（MAC）地址	MAC 地址是用来标识网络节点的硬件地址。
MAC Address Learning	MAC 地址学习	网桥的学习特征，即数据包源地址被记录在桥中。对某一目的地址的数据包只被转发到有记录地址的桥端口上。标有未知地址的数据包被发送到桥的每一个端口。MAC 地址学习能力能减小在相邻局域网的通信量。
MAC Layer	MAC 层	数据链路层的一个子层。
MAN (Metropolitan Area Network)	城域网	覆盖城市或郊区的通信网络。
Mask	掩码	包含或除去某些值的过滤器。例如 IP 地址的子网掩码。
MD5 (Message Digest 5)	消息摘要 5	产生一个 128 比特散列值的算法。MD5 是 MD4 的一 个变种，增加了 MD4 安全信息。MD5 能校验信息的 完整性和原信息的可信度。
MDI (Media Dependent Interface)	介质相关接口	终端站点所使用的电缆。
MDIX (Media Dependent Interface with Crossover)	交叉的介质相关接口	Hub 和交换机使用的电缆。
MDU (Multiply-Divide Unit)	乘除法单元	CPU 内进行乘法和除法运算的高速电路。
MIB (Management Information Base)	管理信息库	MIB 中包含描述网络组件特定状况的信息。
MTU (Maximum Transfer Unit)	最大传输单元	规定可以通过网络传输的最大帧长度。超过最大传输单元的帧必须被分解为较小的帧。
Multicast	组播	发送一个数据包的拷贝到多个端口。
N		
Network Processor	网络处理器	特别为网络和通信功能而优化设计的 CPU 芯片。
NMS (Network Management System)	网络管理系统	网络管理系统是一种接口，它提供一种管理系统的方法。
Node	节点	网络连接终端或多条网络线的交汇点。节点包括： • 处理器 • 控制器 • 工作站
O		
OID (Object Identifier)	对象 ID	在简单网络管理协议（SNMP）中用来识别被管理的对象。在 SNMP 管理者/代理者网络管理范例中，每一个被管理对象必须有对象标识符来得以确认。

OSPF (Open Shortest Path First)	开放最短路径优先	一种 TCP/IP 内部网关协议。它会计算最低开销路径、多路路径和负载均衡。
P		
Packet	数据包	包交换系统中传输的信息块。
PDU (Protocol Data Unit)	协议数据单元	某一层协议中指定的数据单元，包含协议控制信息和该层用户数据。
PING (Packet Internet Groper)	Internet 包探测器	一种检验特定 IP 地址是否可到达的工具。它向特定 IP 地址发出一个数据包，然后等待回应。
Policing	（流量）管制	决定流量水平是否在指定范围之内。流量管制管理一个接口上发送或接收数据的最大流量。
Port	端口	提供连接部件的物理接口，允许微处理器与外围设备之间进行通信。
Port Mirroring	端口镜像	将一个端口接收和发送的数据包的拷贝转发到镜像端口，从而实现对网络流量的监控和镜像。
Port Speed	端口速度	端口速度包括： • 以太网 – 10Mbps • 快速以太网 – 100Mbps • 千兆以太网 – 1000Mbps
PPP (Point-to- Point Protocol)	点到点协议	通过串行链路连接到网络。PPP 在 PC 机和 ISP 之间使用链路控制协议（LCP）建立连接。
Privilege	特权	提供安全相关功能的一个用户授权集合，比如用户对设备的访问权限。
Protocol	协议	规定设备如何通过网络交换信息的一组规则。
Protocol Stack	协议栈	用来提供网络功能的一组协同工作的协议。
Q		
QoS (Quality of Service)	服务质量	QoS 提供包含一系列规则的体系。QoS 允许网络管理员依据优先级、应用类型、源地址和目的地址决定何种网络流量被转发以及如何转发。
Query	查询	从数据库提取信息，并以恰当的方式表示出来以供使用。
R		
RADIUS (Remote Authentication Dial-In User Service)	远程拨入用户认证服务	一种对系统用户进行认证，并跟踪连接时间的方法。
RDP (Remote Desktop Protocol)	远程桌面协议	远程桌面协议允许客户端通过网络与终端服务器通信。
Redundancy	冗余	提供设备、服务或事件的备份。如果一个设备、服务或事件失败，备份可以代替损失的功能。
Relay Agent	中继代理	Internet 上在 DHCP 客户端和服务器之间传递 DHCP 消息的主机或路由器。
RIP (Routing Information Protocol)	路由信息协议	规定路由器之间如何交换路由表信息。

RJ-11 Connector	RJ-11 连接器	压合四条线。RJ-11 连接器可将话筒连接到电话机，还可将电话机连接到墙壁上的电话接口。
RJ-45 Connector	RJ-45 连接器	压合八条铜线并与 RJ-11 连接器的形状类似。RJ-45 连接器通常使用在以太网设备上。
RMON (Remote Monitoring on Network)	网络远程监控	提供从单个工作站收集网络信息的功能。
RTOS (Real-Time Operating System)	实时操作系统	为实时计算机系统设计的操作系统。
Router	路由器	连接不同网络的设备。路由器在两个或者多个网络之间转发数据。路由器工作在第三层。
RSTP (Rapid Spanning Tree Protocol)	快速生成树协议	侦测并利用网络拓扑结构，能加快生成树的收敛，并避免转发环路。
Running Configuration File	运行配置文件	运行配置文件中包含启动配置文件中的所有配置命令，以及在当前会话中输入的命令。如果设备断电或者重启，存储在运行配置文件中的所有配置命令将会丢失。
RSVP (Resource ReSerVation Protocol)	资源预留协议	允许 Internet 应用为网络流量获取不同的服务资源。
S		
Segmentation	分段	将 LAN 分割成不同的网段并用网桥和路由器连接起来。分段消除了 LAN 的带宽局限性。
Server	服务器	为网络上其他计算机提供服务的中心计算机。提供的服务包括存储文件和访问应用程序。
SNMP (Simple Network Management Protocol)	简单网络管理协议	简单网络管理协议用来对 LAN 进行管理。基于 SNMP 的应用程序与设备内置的 SNMP 代理进行通信。SNMP 代理收集网络活动及设备状态相关的信息，发送给管理站点。
SoC (System on Chip)	片上系统	在一片芯片上包含整个系统的专用集成电路。例如，一个应用于电信的 SoC 可包含一个微处理器、数字信号处理器（DSP）、RAM 和 ROM。
STP (Spanning Tree Protocol)	生成树协议	生成树协议能避免网络中产生环路。协议对任意网桥布局都能提供一个树状的拓扑结构，并消除环路，为网络终端站点之间提供唯一一条路径。
SSH (Secure Shell)	安全终端	使用安全终端通过网络登录远程计算机，执行命令，并在计算机之间传输文件。
Stand-alone Mode	独立模式	允许设备独立于其他设备运行。
Startup Configuration	启动配置	启动配置可保存设备在断电或重启之前的配置。
Subnet (Sub-Network)	子网	子网是网络中共享公共地址部分的一部分。在 TCP/IP 网络中，地址前缀部分相同的设备属于同一子网。比如，所有地址形式为 157.100.100.x 设备都是同一子网的部分。

Subnet Mask	子网掩码	子网掩码与 IP 地址进行逻辑与运算以表示子网地址。
T		
TCP (Transmission Control Protocol)	传输控制协议	传输控制协议使两台主机能够通信并交换数据流。TCP 保证数据包的到达，并保证接收到数据包的顺序就是发送它们的顺序。
Telnet	远程登录	使系统用户能够登录远程计算机并使用上面的资源。
TFTP (Trivial File Transfer Protocol)	简单文件传输协议	简单文件传输协议使用 UDP 进行文件传输，并且不提供任何安全特性。
Trap	陷阱	SNMP 送出的消息以表示系统事件的发生。
Trunking	端口汇聚	将一组端口捆绑在一起形成一个聚合组，从而优化了端口的使用。
U		
UDP (User Data Protocol)	用户数据协议	UDP 发送数据包，但是不保证包一定能到达目的地。
Unicast	单播	一种只将一个数据包转发给一个用户的转发形式。
V		
VLAN (Virtual Local Area Network)	虚拟局域网	组成局域网的逻辑子组。VLAN 是由软件而非硬件实现的。
VDSL (Very high bit rate DSL)	超高比特率用户数字用户线	非对称数字用户线的版本之一，用于光纤节点到邻近用户的连接。
W		
WAN (Wide Area Network)	广域网	覆盖大范围地理区域的网络。
Wildcard Mask	通配符掩码	指定 IP 地址中的哪些比特位有用，以及忽略哪些比特位。通配符掩码是 255.255.255.255 时，表示忽略所有的比特位；通配符掩码是 0.0.0.0 时，表示所有的比特位都有用。例如，当目的 IP 地址是 149.36.184.198 而且通配符掩码是 255.36.184.0 时，头两个比特位有用，末尾两个比特位被忽略。

交换机初始配置指南

第1章　交换机初始配置

本章介绍如何通过命令行接口对交换机进行初始配置，包含下列内容：

- 配置终端
- 安装步骤
- 启动交换机
- 配置总览
- 高级配置
- 使用启动菜单

1.1　配置终端

这里所说的“终端”一般就是指 PC 机。将交换机上的 Console 口与 PC 机的串口通过产品附带的串口线连接起来，并在 PC 机上运行“超级终端”程序。“超级终端”的配置如下：

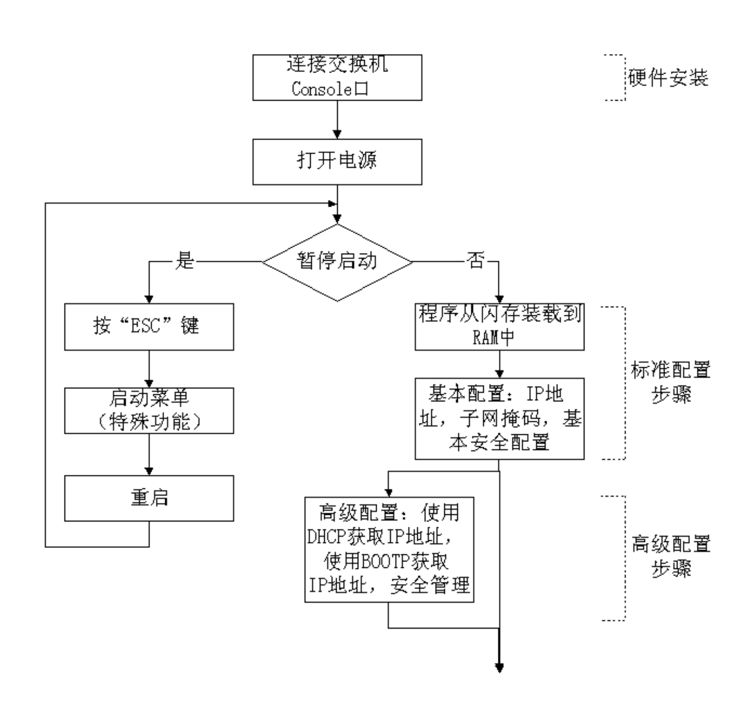
1. 将每秒位数（即波特率）设置为 38400。
2. 将数据位设置成 8，停止位设置成 1，同时奇偶校验选择“无”。
3. 数据流控制选择“无”。
4. 在“超级终端”的属性对话框中将终端仿真模式设置为“VT100”。注意“功能键，箭头键和 Ctrl 键”单选框，需选择为“终端键”（而不是“Windows 键”）。

☞ 注意：

当使用Microsoft Windows 2000 下的超级终端时，确保Windows 2000 Service Pack2 或更高版本已被安装，这样才能保证箭头键在超级终端VT100 虚拟仿真模式下的功能比较正常。若想了解 Windows 2000 Service Pack的更多信息，请登录 www.microsoft.com。

1.2　安装步骤

下图说明了安装及配置步骤。标准配置步骤中包含最基本的交换机配置。高级配置步骤中的功能将在本章的后面部分介绍。



1.3 启动交换机

交换机出厂时没有任何配置。按照以下步骤启动交换机：

1. 按照 1.1 节所述步骤正确设置终端。

2. 连接交换机的电源线，并将 Console 口与 PC 机串口连接。

3. 打开电源。

每次上电时交换机将进行上电自检，在此过程中对硬件进行检测，并判断交换机能否正常工作。如果自检出现问题，程序会挂起，启动过程终止。如果自检通过，将从闪存中装载一个可执行映像到 RAM 中。上电自检信息将在终端上显示出来，指示自检过程中每个检测项目是成功还是失败。

当交换机启动，首先检验交换机存储器可用空间然后继续启动。下面是交换机上电自检过程中在终端上显示的内容：

```
------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test............................PASS

Testing the System SDRAM................................PASS

Boot1 Checksum Test...........................................PASS

Boot2 Checksum Test...........................................PASS

Flash Image Validation Test................................PASS

BOOT Software Version 1.0.0.04 Built  29-Nov-2005  11:56:12

TPLink Switch based on 88E6218 with ARM946E-S.

32MByte SDRAM. I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.

Preparing to decompress...
```

启动过程大概需要 60 秒。

当自检信息中出现“Autoboot in 2 seconds...”这一行时，表明交换机上电自检过程中没有遇到问题。这时如果在 2 秒钟内按 Enter 或者 Esc 键，将打开启动菜单。启动菜单的功能将在 1.6 节中介绍。

如果系统启动过程没有按 Enter 或者 Esc 键，交换机将从闪存中装载程序到 RAM 中，然后从 RAM 中继续运行程序，并显示交换机的端口列表。

交换机成功启动后，将出现系统提示符 console>，表明交换机已准备好接收用户的配置命令。但是在配置交换机前，请确保交换机使用的是最新的软件版本，如果不是，请下载并安装最新版本。关于如何将最新版本的软件下载到交换机上，请参考 1.6.1 节。

1.4 配置总览

在给交换机分配静态 IP 地址之前，请先确认如下信息：

- 将为交换机分配的 IP 地址
- 默认网关地址
- 网络子网掩码

交换机包含两种配置类型：

- 初始配置：包含了基本的配置功能以及基本的安全考虑。
- 高级配置：包含动态 IP 配置和更多的高级安全考虑。

☞ 注意：

修改配置后，在重启交换机前必须对新配置进行保存。如要保存配置，请输入：

```
console# copy running-config startup-config
```

1.4.1 初始配置

在交换机成功启动后才能对交换机进行初始配置，内容包括配置静态 IP 地址和子网掩码，设置用户名和权限以进行远程管理。如果使用基于 SNMP 的管理站点来管理交换机，还必须设置 SNMP 团体名称。

进行初始配置须满足以下条件：

- 交换机在此之前没有进行过配置，即保持出厂时没有任何配置的状态。
- 交换机能成功启动。
- 终端已经连接，并能显示终端提示符（重复按几次 Enter 键来确认提示符显示正确）。
- 交换机没有设置默认用户和密码。

交换机的初始配置将通过串口完成，在初始配置完成后，就可以通过已连接的串口进行管理，或者通过初始配置中指定的端口来远程管理交换机。

初始配置包含下面的内容：

- 设置用户名及其密码，并将该用户特权级设置为最高值 15。
- 配置静态 IP 地址和默认网关。
- 配置 SNMP 读/写团体名称。
- 通过 DHCP 服务器来获取 IP 地址。

在进行交换机的初始配置步骤之前，必须先从网络管理员处获得下列信息：

- 将要分配给默认 VLAN 的 IP 地址
- 网络的 IP 子网掩码
- 默认网关的 IP 地址
- SNMP 团体名称

1.4.1.1 静态IP与子网掩码

IP 地址可以配置在交换机的任意一个端口上。在配置完成之后，建议输入“show ip interface”命令来查看刚刚配置的内容是否正确。

配置交换机所用的命令是与端口相关的。

为了通过远程网络来管理交换机，必须设置一个静态路由，这样当在交换机本身的地址表中找不到数据包所要发送到的 IP 地址时，可以让数据包知道该往哪里发送。路由的 IP 地址必须与交换机管理端口 IP 属于相同网络。

要配置静态路由，可在系统提示符下输入下面的配置实例中所示的命令，将 100.1.1.1 这个 IP 地址分配给 VLAN 1，默认网关设置为 100.1.1.10。注意在默认情况下，VLAN 1 是缺省 VLAN，而且所有端口都是 VLAN 1 的成员。

```
console# configure

console(config)# interface vlan 1

console(config-if)# ip address 100.1.1.1 255.255.255.0

console(config-if)# exit

console# ip default-gateway 100.1.1.10
```

使用下面的命令来确认设置 IP 正确无误：

```
console# show ip interface

IP Address          I/F            Type

-----------------   -----------    -----------------

100.1.1.1/24        vlan 1         static
```

1.4.1.2　给默认VLAN分配静态IP地址

下面的示例使用如下假设：

- 分配给 VLAN 接口的 IP 地址是 192.168.1.123
- 网络子网掩码是 255.255.255.0
- 默认网关的 IP 地址是 192.168.1.1
- 读/写 SNMP 团体名称是“private”

```
console> enable
console# configure
console(config)# username admin password admin level 15
console(config)# interface VLAN 1
console (config-if) # ip address 192.168.1.123 255.255.255.0
console (config-if) # exit
console (config) # ip default-gateway 192.168.1.1
console (config) # snmp-server community private rw
console(config)# exit
console#
```

验证 IP 和默认网关地址

为确保 IP 地址和默认网关被正确分配，执行下面命令并且检查输出信息：

```
console# show ip interface
Gateway IP Address            Activity status
--------------------------------------------------------
----                          ---
192.168.1.1                   Active

IP address                    Interface                 Type
------------------            ----------------          --------
192.168.1.123/24              VLAN 1                    Static
```

1.4.1.3 用户名

设置用户名后就可以远程管理交换机，例如通过 SSH，Telnet 或者 Web 界面。要获得交换机的完全管理权限（超级用户），必须指定最高特权级 15。

☞ 注意：

只有拥有最高特权级 15 的用户(超级用户)才能通过Web界面来管理交换机。

要想了解更多管理权限信息，请查看《CLI 参考指南》。

配置成功的用户名可作为远程管理会话的登录名。要配置用户名和权限，可参照下列配置实例，在系统提示符下输入命令：

```
console> enable
console# configure
console(config)# username admin password admin level 15
```

1.4.1.4 SNMP团体名称

简单网络管理协议（SNMP）提供管理网络设备的方法。设备会运行被称为 SNMP 代理的内置软件，它会维护一组用来管理设备的变量。这些变量集合在一起保存在管理信息库（MIB）内部，并可通过 SNMP 代理去访问。SNMP 代理定义了 MIB 内数据的格式，并定义了通过网络访问这些数据的格式。

访问字符串和 SNMP 团体名称控制了对 SNMP 代理的访问权限。

本系列交换机完全兼容 SNMP 协议。交换机内置的 SNMP 代理支持一组标准的和私有的 MIB 变量。要开发一个管理站点，开发者必须了解 MIB 中数据树的确切结构，并在开始管理 MIB 前获取完整的私有 MIB 信息。

除了 SNMP 管理站点的 IP 地址和团体（包括团体名称和访问权限），所有的参数都可以在 SNMP 管理平台上进行管理。如果不存在团体名称，将不能通过 SNMP 管理访问交换机。

☞ 注意：

交换机设备出厂时，没有配置团体名称。

在实际应用中，通常情况下可为交换机设置两个团体名称，一个是公共团体名称，具有只读访问权限；另一个是私有团体名称，具有读 / 写访问权限。公共名称允许授权管理站点只读地获取 MIB 对象，而私有名称允许授权管理站点获取和修改 MIB 对象。

在初始配置过程中，可以根据网络管理员的需要对交换机进行配置，并与 SNMP 管理站点的使用相协调，还可以对团体名称，团体访问权限和 IP 地址进行配置。

SNMP 设置选项有：

- 团体名称
  - 只读：指出团体成员能浏览配置信息，但是不能修改任何信息。
  - 读/写：指出团体成员能浏览和修改配置信息。
  - 超级：指出团体成员具有管理员访问权限。
- 配置 IP 地址如果 IP 地址没有配置，所有具有相同团体名称的团体成员都具有相同的访问权限。

按照下列步骤配置 SNMP 站点 IP 地址和团体名称：

1. 在用户模式提示符下，输入 enable 命令，将进入特权模式，命令行提示符变成#。
2. 输入 configure 命令后按 Enter 键进入配置模式。
3. 在配置模式下，输入 SNMP 配置命令，参数包括团体名称（私有），访问权限（读和写）和 IP 地址，如下面实例：

```
console# configure

console(config)# snmp-server community private rw 11.1.1.2
console(config)# end
console# show snmp
Community-String               Community-Access              IP address
--------------------------------   -----------------------------------   -----------------------
private                        readWrite                     11.1.1.2
Traps are enabled.
Authentication-failure trap is enabled.

......

System Contact:
System Location:
```

以上过程通过本地终端完成了对交换机的初始配置，这样就能通过远程登录来对交换机进行进一步配置。

1.5 高级配置

本节介绍 IP 地址的动态分配，以及基于认证，授权和统计机制的安全管理，包含的内容如下：

- 从 DHCP 服务器上获取 IP 地址
- 从 BOOTP 服务器上获取 IP 地址
- 安全管理和密码设置

当通过 DHCP 和 BOOTP 服务器获取和设置 IP 地址时，从服务器获取的配置包括 IP 地址，可能还包括子网掩码和默认网关。

1.5.1 从DHCP服务器上获取IP地址

当交换机使用 DHCP 协议获取 IP 地址时，它将作为一个 DHCP 客户端。按照以下步骤操作以从 DHCP 服务器获取 IP 地址：

1. 将任意端口连接到 DHCP 服务器或者是一个架设了 DHCP 服务器的子网。

2. 输入以下命令用已选择的端口获取 IP 地址。下面的例子中，所示的命令是基于配置所使用的端口类型。

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address dhcp hostname admin-host
console(config-if)# exit
console(config)#
```

3. 如果要验证是否已经正确获取 IP 地址，在系统提示符后中输入如下所示的

show ip interface 命令：

```
console# show ip interface
IP Address             I/F            Type
--------------------   ---------------   --------------
100.1.1.1/24           vlan 1         dynamic
```

☞ 注意：

- 从DHCP服务器获得一个新的IP地址前不必删除交换机已有的配置。
- 复制配置文件时，应避免使用包含有启用已经连接到相同的DHCP服务器接口的DHCP项的指令的配置文件，或者是移动到有相同设置的配置文件。如果这样做了，交换机会在新的配置文件中启用DHCP项，DHCP又会引导交换机重新装载相同的文件。

1.5.2 从BOOTP服务器获取IP地址

交换机支持标准的 BOOTP 协议，BOOTP 协议能够使交换机自动从网络中任意标准 BOOTP 服务器上下载 IP 主机设置。这种情况下，交换机将作为一个 BOOTP 客户端。

如何从 BOOTP 服务器上获取 IP 地址：

1. 选择任意端口连接至 BOOTP 服务器或者是架设了 BOOTP 服务器的子网。
2. 在系统提示符下，键入 delete startup-config 命令从闪存中删除相应的启动配置。然后在无配置的条件下重新启动，交换机将在 0 秒内发出 BOOTP 请求，并将会自动获取 IP 地址。

☞ 注意：

当交换机重新启动时，任何ASCII终端或者是键盘的输入都会自动取消未完成的BOOTP进程，交换机将不会从BOOTP服务器上获得IP地址。

下面的例子详细说明了这个过程：

```
console> enable
console# delete startup-config
Startup file was deleted
console# reload
You haven't saved your changes. Are you sure you want to continue  (Y/N)[N]?
This command will reset the whole system and disconnect your current session. Do you want to continue (Y/N)[N]?
*****************************************************
*****************  SYSTEM RESET  *****************
*****************************************************
```

3. 如果要验证是否已经正确获取 IP 地址，同样可在在系统提示符后中输入 show ip interface 命令。

1.5.3 安全管理和密码设置

系统安全通过 AAA（认证，授权和统计）机制来实现，它管理着用户的访问权限，特权级和管理方式。AAA 使用本地和远程用户数据库，数据的加密通过 SSH 机制完成。

交换机出厂时没有默认密码设置，所有的密码都是由用户来设定。当用户的自定义密码丢失时，可以通过本地终端从启动菜单中调用密码恢复程序（请参考 1.6.3 节）。执行这个程序后，允许本地用户在下一次登录时无需输入密码。

1.5.3.1 设置安全密码

可以为以下服务设置安全密码：

- Console
- Telnet
- SSH
- HTTP
- HTTPS

☞ 注意：

当创建一个用户时，默认的特权级是 1，该特权级用户只能访问但是没有更改配置的权限。特权级为 15 的用户拥有访问和修改交换机配置的权限。虽然用户可以被设定成拥有 15 的特权级并且密码为空，但是推荐的设置是需设定一个密码。如果没有设定密码，则拥有特权级 15 的用户可以使用任何密码访问WEB界面。

1.5.3.2 设置初始控制台（Console）密码

设置一个初始的控制台密码，输入以下命令：

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password george
```

如上设置之后，再通过控制台登录交换机时，在密码提示符处输入密码 george。

当进入特权模式时，同样在密码提示符处输入密码 george。

1.5.3.3 设置初始Telnet密码

设置一个初始 Telnet 密码，输入以下命令：

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
```

如上设置之后，再通过 Telnet 登录交换机时，在密码提示符处输入密码 bob。

当更改交换机的启动模式时，同样在密码提示符处输入密码 bob。

1.5.3.4 设置初始SSH密码

设置一个初始的 SSH 密码，输入以下命令：

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password jones
```

如上设置之后，再通过 SSH 登录交换机时，在密码提示符处输入密码 jones。

当更改交换机的启动模式时，同样在密码提示符处输入密码 jones。

1.5.3.5 设置初始HTTP密码

设置一个初始的 HTTP 密码，输入以下命令：

```
console(config)# ip http authentication local
console(config)# username admin  password user1 level 15
```

1.5.3.6 设置初始HTTPS密码

设置一个初始的 HTTPS 密码，输入以下命令：

```
console(config)# ip https  authentication local
console(config)# username admin password user1 level 15
```

当设置成使用 HTTPS 时，输入以下命令：

```
console(config)# crypto  certificate 2 generate key_generate
console(config)# ip https  server
```

如上设置之后，当初次启用 HTTP 或者 HTTPS，输入用户名 admin 密码 user1。在 WEB 浏览器中启用 SSL 2.0 或以上版本以显示页面的内容。

☞ 注意：

HTTP和HTTPS服务需要 15 的特权级并且直接连接至可配置级的访问权限。

1.6 使用启动菜单

在启动过程中可以调出启动菜单，该菜单中的项目包括软件下载，擦除闪存以及密码恢复。诊断模式只供技术支持人员使用，本文档中不包括这方面内容。

当交换机启动时，在上电自检完成后通过用户输入就可以进入启动菜单。下面是详细步骤：

1. 打开交换机电源，观察启动信息：

```
------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test............................PASS

Testing the System SDRAM................................PASS

Boot1 Checksum Test..........................................PASS

Boot2 Checksum Test..........................................PASS

Flash Image Validation Test................................PASS



BOOT Software Version 1.0.0.04 Built  29-Nov-2005  11:56:12


TPLink Switch based on 88E6218 with ARM946E-S.
32MByte SDRAM. I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

2. 当出现自动引导信息时，按 Enter 键或者 Esc 键以显示启动菜单：

```
[1]  Download Software

[2]  Erase Flash File

[3]  Password Recovery Procedure

[4]  Enter Diagnostic Mode [5]  Set Terminal Baud-Rate [6]  Back

Enter your choice or press 'ESC' to exit:
```

启动菜单里的项目可以通过在 ASCII 终端或者是 Windows 的超级终端中输入相应命令来执行。以下部分将说明启动菜单中可用的选项。

☞ 注意：

在启动菜单中选择选项时，如果在 15 秒内没有进行任何选择，就会超时而继续系统引导过程。由于只有技术支持人员可以使用诊断模式，本文档将不对诊断模式进行描述。

1.6.1 软件下载

[选项 1]当必须下载新版本软件来替换被破坏的文件或者是系统软件需要升级的时候，需要执行软件下载程序。按照下面的步骤从启动菜单中执行下载软件程序：

1. 在启动菜单中，按 1 并按 Enter 键，会出现以下提示信息：

```
Downloading code  using XMODEM
```

2. 当使用超级终端时，在超级终端菜单条上选择“传送 → 发送文件”。

3. 在文件名输入框中，输入欲下载的文件路径。

4. 确认在协议中选择了 Xmodem 协议

5. 按“发送”按钮，开始软件下载。

☞ 注意：

- 软件下载完成后，交换机将自动重启。
- 软件下载也可以通过TFTP来进行。

1.6.1.1 通过TFTP服务器来下载软件

这部分包含从 TFTP 服务器下载交换机软件（包括系统程序映像和引导程序映像）的说明。在下载软件之前需要先设置 TFTP 服务器。本部分包含以下主题：

- 系统程序映像下载
- 引导程序映像下载

系统程序映像下载

当交换机启动时，它会将存储在闪存中的当前活动的系统程序映像装载到内存中，并解压运行。当下载一个新映像时，下载的映像将被存储在用于映像备份的闪存区域中。在下一次启动的时候，交换机将装载和运行当前活动的系统程序映像，除非设定新的映像为当前活动映像。

按照下面的步骤通过 TFTP 服务器来下载一个系统程序映像：

1. 确认交换机的其中一个端口已经设置了 IP 地址，并且通过该 IP 可以 ping 通 TFTP 服务器。

2. 确认 TFTP 服务器上存有要下载的文件。

3. 输入 show version 命令来查看当前交换机正在运行的软件的版本，以下是一个显示版本信息的例子：

```
console# show version

SW version    1.0.0.30 ( date  16-Jul-2006 time  09:19:44 )
Boot version    1.0.0.04 ( date  29-Nov-2005 time  11:56:12 )
HW version    01.00.00
```

4. 输入 show bootvar 命令来显示当前活动的系统映像，下面例子是所显示的信息：

```
console# sh bootvar

Images currently available on the FLASH
Image-1 active (selected for next boot)
Image-2 not active
console#
```

5. 输入 copy tftp://{TFTP 服务器地址}/{文件名} image 命令来拷贝新的系统程序映像到交换机。当一个新的映像下载后，它将被存储在当前非活动的映像区域（因为第 4 步中显示当前非活动的映像是 image-2，所以新下载的映像将会保存在 image-2 区域，原有的 image-2 中的内容将会被覆盖）。下面的例子是所显示的相关信息：

```
console# copy tftp://176.215.31.3/file1.ros image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 3172288 bytes copied in 00:01:48 [hh:mm:ss]
```

感叹号表明正在进行复制，每一个感叹号代表成功传送 512 字节。一个句点表示复制进程超时，一行中出现许多句点表示复制进程失败。

6. 如果要在下次启动时让交换机启动刚下载的系统程序映像，必须使用 boot system image-2 命令将当前活动映像切换到 image-2。命令执行时的信息如下所示：

```
console# boot system image-2
```

7. 输入 reload 命令，下面的是显示的信息：

```
console# reload

This command will reset the whole system and  disconnect your current session. Do you want to
continue (Y/N) [N]?
```

8. 输入 y，交换机将会重启。

引导程序映像下载要更新引导程序映像，需从 TFTP 服务器上下载新的引导程序映像并写入闪存中。当交换机开机时，引导程序映像将会被加载。

从 TFTP 服务器上下载一个引导映像的步骤：

1. 确认交换机的其中一个端口已经设置了 IP 地址，并且通过该 IP 可以 ping 通 TFTP 服务器。

2. 确认 TFTP 服务器上存有要下载的文件。

3. 输入 show version 命令来查看当前交换机正在运行的软件的版本，以下是一个显示版本信息的例子：

```
console# show version
SW version    1.0.0.30 ( date  16-Jul-2006 time  09:19:44 )
Boot version    1.0.0.04 ( date  29-Nov-2005 time  11:56:12 )
HW version    01.00.00
```

4. 输入 copy tftp:// {TFTP 服务器地址}/{文件名} boot 命令来复制启动程序映像到交换机，下面的例子是显示的信息：

```
console# sh bootvar
Images currently available on the FLASH
Image-1 active (selected for next boot)
Image-2 not active
console#
```

5. 输入 reload 命令，下面的是显示的信息：

```
console# reload

This command will reset the whole system and  disconnect your current session. Do you want to continue (Y/N) [N]?
```

6. 输入 y，交换机将会重启。

1.6.1.2 通过Xmodem协议来下载软件

这部分主要讲解使用 Xmodem 下载交换机软件（包括系统程序映像和引导程序映像）。Xmodem 是一个用于更新备份配置文件的数据传输协议。

引导程序映像下载

使用 Xmodem 下载引导程序映像的步骤如下：

1. 输入命令 copy xmodem:boot，交换机就会准备好通过 Xmodem 协议接收映像文件。命令显示以下信息：

```
console# copy xmodem: boot
Please download program using XMODEM. console#
```

2. 在 20 秒内按照 1.6.1 节开始处所示的方法从超级终端上使用 Xmodem 协议发送需要下载的映像。如果 20 秒内没有开始发送，则命令就会超时。

系统程序映像下载

使用 Xmodem 下载系统程序映像的步骤如下：

1. 输入命令 copy xmodem:image，交换机就会准备好通过 Xmodem 协议接收映像文件。命令显示以下信息：

```
console# copy xmodem: image
Please download program using XMODEM
```

2. 同样按照 1.6.1 节开始处所示的方法从超级终端上使用 Xmodem 协议发送需要下载的映像。

1.6.2 擦除闪存文件[选项 2]

在某些情况下，需要进行系统配置擦除。如果系统配置被擦除，则通过命令行接口（CLI），内置 WEB 界面（EWS）和 SNMP 配置的所有参数都需要重新设置。

擦除交换机配置的步骤如下：

1. 从启动菜单中，按 2 并按 Enter 键来擦除闪存文件。以下是显示的信息：

```
Warning!About to erase a Flash file.
Are you sure (Y/N)? y
```

2. 按下 y，显示以下信息：

```
Write Flash file name (Up to 8 characters, Enter for none.):config
File config (if present) will be erased after system initialization
======== Press Enter To Continue ========
```

3. 输入 config 作为闪存文件的名字，配置将会被擦除，交换机将重启。

4. 恢复交换机的初始配置。

1.6.3 密码恢复[选项 3]

如果密码遗失，可以在启动菜单中执行密码恢复程序。执行这个程序后，允许本地用户在下一次登录时无需输入密码。

恢复密码的步骤如下：

1. 在启动菜单中，按 3 并按 Enter 键，密码会被删除。

☞ 注意：

为保证交换机的安全，删除密码后请重新设置各种管理方式的密码。

1.6.4 进入诊断模式[选项 4]

诊断模式只供技术支持人员使用。

1.6.5 设置终端波特率[选项 5]

设置终端波特率的步骤：

1. 在启动菜单中，按 5 并按 Enter 键。
2. 可选的波特率值为 2400、4800、9600、19200、38400，输入波特率，或按 Esc 键退出。
3. 按下 Enter 键，完成波特率设定。